cenfri

BANKSERVAFRICA

ID proxy initiatives across the globe

An analysis

November 2019

Authors

Barry Cooper

Laura Muñoz Perez

Antonia Esser

Michaella Allen

Nolwazi Hlophe

Matthew Ferreira

Cenfri

Tel. +27 21 913 9510
Email: info@cenfri.org
The Vineyards Office Estate
Farm 1, Block A
99 Jip de Jager Drive
Bellville, 7530
South Africa

PO Box 5966
Tygervalley, 7535
South Africa

www.cenfri.org

Foreword by BankservAfrica

A transformed payments ecosystem is imminent in South Africa. Following the impetus created by the South African Reserve Bank's Vision 2025, BankservAfrica and the Payments Association of South Africa, together with the South African payments industry, have been clarifying and defining a plausible path for transformation in South Africa. Beginning in 2017 with the joint BSA-PASA research programme that produced our 3-part study of modernization efforts world-wide (brought together under the heading "Modernising Payments Systems" and available on our web-site), BankservAfrica has taken a key role in providing research to the industry that it topical, pertinent, and applicable.

In the last year, the South African payments industry has increasingly shifted its focus towards instant payments for the digitally connected economy, while addressing the persisting issue of financial inclusion in South Africa. Through extensive work done in the industry, co-ordinated and facilitated by the Payments Association, proxy and addressing services have been identified as a critical lever for adoption of instant or near-instant payments services. Proxy services allow payments to be successfully made using only an agreed identifier, such as mobile number, or a national identity number. By doing so, they remove much of the consumer friction currently associated with electronic payments. When coupled to a real-time clearing option, the potential for adoption grows exponentially. However, of greater interest in South Africa is that the combination of such services promises to penetrate markets traditionally resistant to digitisation, advancing financial inclusion.

For all these reasons, proxy and addressing services are a subject of intense discussion in South Africa right now. But what kinds of proxies should be used? How should they be combined? What are the risks and rewards associated with each? More prosaically, what does this mean for the spaza shop owner who relies on cash and does not own a bank account?

As part of our growing library of payments thought leadership, BankservAfrica has commissioned research with the Cenfri, aimed at clarifying and enabling this critical dialogue. We look at proxy initiatives on the African continent and elsewhere, and provide both a direction of analysis, and a framework for evaluation of different approaches. In so doing, we identify the central criteria set that proxy services need to meet - accessibility, verifiability and security, trustworthiness, uniqueness, privacy, customer experience and cost - and give examples of their use that are applicable to the South African industry.

We are extremely pleased to make this analysis available and hope it makes a meaningful contribution towards a transformed South Africa.

Table of contents

List of tables

List of figures

List of boxes

List of acronyms and abbreviations

ABIS	automatic biometric identification system
ABN	Australian Business Number
AEPS	Aadhaar Enabled Payment System
API	application programme interface
APBS	Aadhaar Payment Bridge System
ASAs	authentication service agencies
BHIM	Bharat Interface for Money
BIC	European Business and Innovation Centre
BSB	Bank State Branch
BVN	bank verification number
CBN	Central Bank of Nigeria
CIDR	central identities data repository
CoDi	Cobro Digital
EFT	electronic funds transfer
eKYC	electronic know-your-customer
EMV	Europay, MasterCard and Visa
FSP	financial service provider
FSS	fast settlement service
GDPR	general data protection regulation
HMAC	hashed message authentication code
IBAN	international bank account number
IIN	institution identification numbers
IMEI	international mobile equipment identity
KYC	know-your-consumer
MPL	mobile proxy look-up service
MSD	magnetic stripe data
MSISDN	mobile station international subscriber directory number
MST	magnetic stripe technology
MTO	money transfer operator
NFC	near-field communication
NIBSS	Nigeria Inter-Bank Settlement System
NIN	national identity number
NPCI	National Payments Corporation of India

NPP	new payments platform
NPPA	New Payment Platform Australia
OrgID	organisation ID
OTP	one-time password
P2B	peer -to -business
P2P	peer-to-peer
POI	point of interaction
POS	point of sale
PSP	payment service provider
RBA	Reserve Bank of Australia
RTGS	real-time gross settlement
RTP	request-to-pay
SEPA	Single Europe Payment Area
SPEI	Interbank Electronic Payment System
STR	suspicious transaction report
TARGET2	Trans-European automated real-time gross settlement express transfer system
TIPS	TARGET instant payment settlement
UIDAI	unique identification authority
UPI	unified payments interface
USSD	unstructured supplementary service data
VID	virtual ID

1. Introduction

Real-time instant payments have become a hallmark of any modern digitally connected economy and financial system. It enables consumers to make individual payments, account-to-account, within seconds at any time of the day, and be accredited to beneficiary accounts at any time, in addition i.e. 24/7/365. For banks, instant payments promise greater cost-savings by replacing expensive legacy payment methods or schemes; wider availability of credit; and improved value-add to consumers demanding payment services with greater speeds, convenience, and security (KPMG, 2017). With over 60% of the population formally banked and an increasingly universal Smartphone penetration, South Africa is primed for the introduction of a simple, low-cost, low-value instant payments service and its benefits for both commercial and public sector use cases (World Bank, 2018).

In light of this, African banks are increasingly looking to create new real-time instant payment retail offerings. A viable proposition for these instant retail payment services however requires the establishment of a consumer quality assurance scheme such as central proxy identification systems.

A proxy-enabled registration system is a core part of the development of any real-time payment offering. The use of a proxy as a payment destination or payment initiation mechanism implies that the beneficiary has registered a unique proxy and can trigger a payment initiation request based on this proxy identifier. A robust and efficient proxy registration system is vital to the success of an instant payment system, as it not only enables consumers to transact more seamlessly without the need to register a beneficiary with a bank name, bank account number or branch code, but, in addition, provides payer confirmation of beneficiary details. Furthermore, if sufficiently robust, proxy systems can be key in defending against reverse look-up attack; automated skimming of consumer information; incidences of false positive beneficiary identification and fraud, more broadly, in a system potentially vulnerable to rapid interception of account information and theft.

Box 1: South Africa as a case study for identification and identity proxies

In South Africa, the base identifier is the National Identity Smart Card which is linked to the Home Affairs database. It contains 10 fingerprints biometrics in the 4-4-2 formation. In addition to the NID Smart Card, there are other foundational identifiers for South Africans or people living in South Africa, such as the South African passport, the national driving licence, and an international passport. These documents are considered base identity documents in the FICA guidance and are therefore necessary and robust for KYC and payment identification purposes.

Base or reference identities can be thought of as the underlying verified identity that forms the foundation of any proxy identifier.

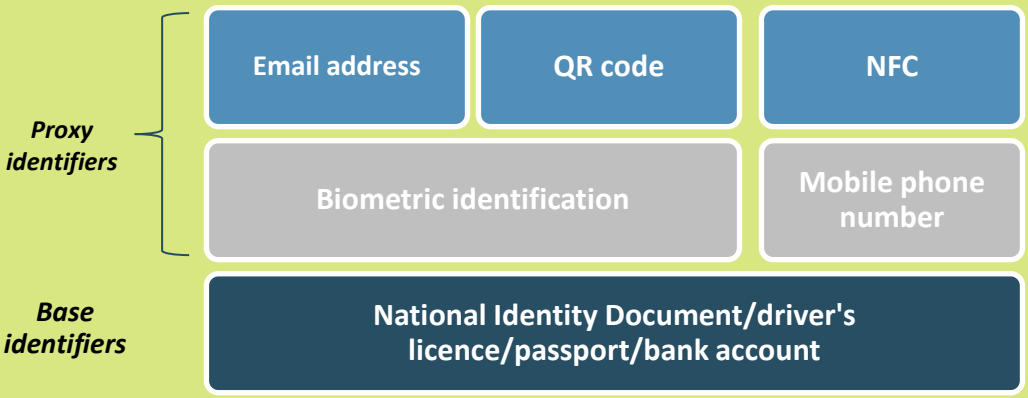

Figure 1. Foundational and proxy identifiers

Source: Authors' own

For example, as depicted in Figure 1. Foundational and proxy identifiers, base identity documents, if linked with biometrics either on the home affairs database or on the bank's database, can serve as primary identifiers linked to proxy identifiers. Traditionally, the bank account number would be the proxy identity number. However, other proxies can be used, such as email addresses, mobile phone numbers, QR codes or NFC. The combination or layering of multiple proxies creates a "stack" that can ensure the robustness of a proxy registration system and the overall effectiveness of a rapid payment system in terms of consumer convenience in making payments. For example, when wanting to make rapid payments, South Africans could utilise these proxy identifiers instead of the current requirement for bank account numbers, given that proxy identifiers are also verifiably linked to the foundational identifiers described above.

Verifying that the proxy identifier is indeed linked to the same person can be done through a variety of methods (Sharma, 2018). Biometrics (selfies and fingerprints) can be used where smart phone capabilities are aligned. SMS and OTP verification as well as USSD codes can be used for smart verification where other techniques like biometrics are not available.

Proxy identities can be held on centralised or decentralised databases that are encrypted. Citizens should have access and the ability to edit data as it changes over time. This is in line with international standards on good ID and privacy protection.

Against this background, this report aims to conduct a landscaping analysis of some of the most prominent ID proxies found internationally and to unpack their respective advantages and disadvantages. This study is performed with the ultimate objective to understand the viability of each proxy system for real-time payment systems within the South African context.

Approach

To explore and understand the various proxy systems currently in place internationally, a case study approach is applied. Nine case studies were chosen based on their uniqueness model type in terms of main proponent of initiative (bank vs. regulator vs. private); and distinct use case[1]. The information and analysis contained in this report is based primarily on desktop research, industry consultation, and stakeholder interviews. The resultant information was synthesised and developed into a report.

Analysis of each proxy system and case study example is assessed according to four key considerations, as suggested by industry leaders and secondary research[2]:

- ***Accessibility***: to attract the maximum number of people or new payment traffic to the system, consumers must have ready access to the proxy identifier(s).
- ***Verifiability***: the proxy must be verifiable through another proxy channel or medium to validate it. Thus, a secondary means of verifying or triangulating the link between the proxy and account holder is important, especially in contexts where there is no single national identity database.
- ***Trust*****:** equally importantly, consumers must trust the validity or have a perceived sense of reliability, regarding the proxy[3]. The literature and also consultations suggest that a trusted proxy needs to be unique to each customer, must protect consumer privacy and must facilitate a friendly and seamless customer experience.
- ***Implementation cost and infrastructure requirements:*** these will be evaluated across all nine case studies as overarching criteria.

As a result, five proxy systems have been selected based on their potential for enhancing access, verifiability, and trust. These identity proxies include:

- Mobile telephone number
- Email address
- QR code
- Near Field Code
- Biometric identification

Structure of the report

The structure of this report is as follows:

- Section 2 contains a discussion of each of the five proxy identifiers and provides an overview of their broad respective benefits and shortcomings along the three considerations of access, verifiability, and trust. Case studies which pertain to given proxies are incorporated to assess their advantages and disadvantages in a real-world and context-specific application.

[1] Please see Appendix A for a breakdown of the case study selection criteria.
[2] Several secondary studies were consulted to further our understanding of the international landscape of ID proxies. Key sources include Banco De Mexico, Lipis IQBusiness, BankservAfrica, PASA, Telecom Regulatory Authority of India, AFI, World Bank and Stats SA.
[3] Apart from objective system reliability, consumer perceptions of reliability can also influence the level of trust in the system. Gauging perceptions would require demand-side research and is outside the scope of the current study.

- Section 3 of the report concludes with final thoughts regarding the relevance and suitability of given proxy systems for the South African context.

2. ID proxy landscape

This section unpacks each proxy by providing (i) a basic description of the proxy and its corresponding user journey before evaluating the proxy according to (ii) its accessibility and iii) the four trust elements introduced above, namely uniqueness, privacy, and customer experience. Relevant case studies are further included to highlight the outcomes of their real-world application.

2.1. Mobile phone number

Key advantages:
- High levels of accessibility among the population
- User-friendly with regard to inputting bank account details

Key disadvantage:
- Multiple hurdles and risks regarding multiple sim cards & recycled phone numbers. Multiple users on one sim card suggest the need for mobile number proxies, ideally to be coupled with other identifiers or proxies

What does the proxy entail?

Mobile number replaces bank account number as identifier. A mobile number ID proxy uses an individual's mobile number instead of the individual's bank account number as an identifier. In some jurisdictions, the mobile number may also be the account number, in which case the individual only has one identifier (Diaz, 2018)[4].

Mobile as anchor throughout user journey. Using the mobile number as a proxy requires the individual to register their mobile number with the financial institution and link it to their account. Thereafter, the mobile number, rather than the underlying bank account number, is used to initiate payment or other account instructions, as well as to receive transaction notifications or account updates[5].

[4] As would be the case for mobile money accounts in some jurisdictions in sub-Saharan Africa.
[5] For example: if an individual wishes to make a payment to another individual, they will enter the mobile number in place of the bank account number. The system may still prompt confirmation of the receiver's name and bank name for transaction validation and the payer will still be required to enter their PIN and, if applicable, a system-generated one-time password to affect the payment. Thus, the mobile number is only the initial identifier in lieu of a bank account number, and not the only number used in the transaction.

How accessible is it?

Ubiquitous. In most economies, there is high penetration of mobile phones[6]. This makes mobile phone numbers one of the most accessible ID proxies and facilitating broad participation in the payment system. Moreover, mobile phone numbers are more readily at hand than bank account numbers, since most people would have the phone numbers of their contacts saved on their phones.

Not suitable in all contexts. In some developing economies, limitations in mobile connectivity infrastructure may constrain accessibility[7], as would KYC barriers to SIM card registration[8]. These potential barriers do not apply in South Africa.

Is it verifiable?

Second medium verification possible. The customer identity linked to the mobile number is verifiable against the MTO routing back-end system or third-party databases (such as a national identity database or the RICA[9] SIM card registration database in SA). The mobile number proxy is compatible with SMS, USSD, voice (alone or with a thin SIM), or API communications or validation systems.

How trustworthy is it?

Uniqueness

Consistency over time for most consumers. In most developed economies, people keep the same phone number for a long time, even after changing the phone device many times. Moreover, phone devices and phone numbers are rarely shared. Those attributes make mobile phone numbers a unique identifier. In the case of South Africa, where number portability applies, a significant portion of the financially active banked population may fall into this category. Additionally, the robustness and uniqueness of mobile phone as an ID proxy can be underpinned by the physical mobile phone device through their international mobile equipment identity (IMEI) number and/or biometric information[10].

Not guaranteed. Uniqueness is not guaranteed for mobile proxies. Where individuals do change their mobile number[11], a mobile number proxy could result in payments or receipts being made to the "wrong" number. A mobile number proxy may also be problematic where it is common practice, as is the case in many developing countries, for one person to use multiple SIM cards, as more than one person (typically family members) use the same SIM

[6] In advanced economies, there is moreover broad access to 4G/5G, a good likelihood of unique numbers, high digital and financial literacy and willingness to engage with digital financial services (DFS).
[7] If a country looking to implement a mobile number ID proxy has a low score in the mobile connectivity index, it may imply that they have limited infrastructure to support adequate spectrum and coverage, limited affordability, consumer readiness and content. For more on the mobile connectivity index, see: GSMA, *The Mobile Connectivity Index*, 2017. Available Online [28 May 2019] https://www.gsma.com/mobilefordevelopment/resources/mobile-connectivity-index/
[8] Where people do not have the required documentation for SIM card registration, a mobile number proxy would imply that they are excluded from the payment system. However, we argue that such barriers would not be any higher than KYC access barriers to opening bank accounts .
[9] Regulation of Interception of Communications and Provision of Communication-Related Information Act
[10] For example, in Nigeria, every transaction is sent to the Telco provider, which checks if the mobile phone number corresponds to the SIM card and to the physical phone device that is registered in the name of the account holder. If the IMEI number is not validated, the transaction will not go through.
[11] This may be done for any of a number of reasons. In South Africa, some of the reasons for changing mobile phone numbers include indebted people trying to avoid being harassed by their banks or people changing their phone numbers after their number has been fraudulently subscribed to WASP.

card, where family members continue to use the phone number of a deceased person, or where people use their SIM card to access a communal or shared device. Insufficient oversight of SIM card registration processes could also undermine uniqueness, for example where vendors or retailers RICA multiple SIM cards. Typically, vendors use family members or a single individual to provide KYC documentation for the SIM card sales stock. Furthermore, the uniqueness of a mobile phone number as identifier may be undermined if SIM cards remain linked to previous users even after the number is assigned to a new person.

Where individuals hold multiple accounts at different financial institutions but have only one mobile number, the individual is forced to choose only one account to receive default payments. Alternatively, other mechanisms have been encountered in case studies where the institution and mobile number together form a combined proxy, but the customer experience could be undermined.

Privacy

Facilitates privacy of account details. The use of a mobile number as an ID proxy shields the underlying account details. As discussed under verifiability, the mobile number may be underpinned by another proxy to ensure robustness, whilst still maintaining accessibility at the front end.

Privacy undermined by phone-sharing, fraud, or cybercrime. In most developed economies, phone devices and phone numbers are private and rarely shared, which makes the mobile phone number a sufficiently private ID proxy. However, where mobile phone-sharing is prevalent, privacy of confirmation text messages would be undermined in the case of a mobile phone proxy. Privacy may also be undermined by fraud or cyber-attacks. Should fraudulent access be obtained to a swapped SIM card, the underlying financial transaction information details would also be compromised[12].

Customer experience

Familiarity boosts customer experience, but some user frustrations may still arise. People are used to using their mobile phones in their everyday life, which makes the mobile number a user-friendly ID proxy. However, the use of mobile proxies is not necessarily always seamless for customers. To overcome the uniqueness challenges highlighted above, most mobile proxy payment systems prompt users for additional information about the receiver (name, bank, etc.) to validate the transaction. Moreover, when an individual loses or replaces their mobile phone, it would require them to re-register their mobile phone number to keep on accessing the underlying bank account.

[12] SIM swap concerns have been raised in Nigeria, where there have been instances of simple SIM swaps in which a phone holder/user approaches a service provider and requests a new SIM with the excuse of having lost the phone. Once in possession of an irregular SIM card, the real owner's SIM card is blocked. From that moment on, the fraudster would have access to all financial transactions and related information on that mobile number proxy. More complex SIM swapping or cloning can occur through the fraudulent abuse of telco backhaul channels. This raises privacy concerns. Regulation has since been strengthened to ensure service providers require credentials and an affidavit before replacing the SIM card, but the threat still remains.

Case study 1: MTN Mobile Money

Context

Introduction of MTN mobile money. MTN Mobile money (MoMo) was introduced in 2005 in South Africa through a joint venture firm set up by Standard Bank, South Africa and MTN (Saji, 2008). It is currently available in 14 countries across Africa, as shown in **Error! Reference source not found.**. The mobile money ecosystem is made up of

Regulators: Financial Services Regulator, Financial Intelligence Unit, Communications Regulator and the Central/Reserve Bank

Operational ecosystem: Mobile money customer, mobile money agent, mobile money service provider and the commercial banks.

Enabling a regulatory environment is critical for mobile money success. The regulatory environment for mobile money services has a strong impact on whether a provider can enter the market and sustainably provide services; determine the best solution to become interoperable; and provide a broad range of services that create value for its customers. Enabling regulation positively influences the growth of mobile money services (GSMA, 2016).

The prudential regulations of mobile money providers effectively mitigate the risk of mobile money customers losing money they have stored in the system.

Regulation requires proportionate AML/CFT controls, such as, allowing for tiered accounts in countries that do not have a universal ID system and for remote account opening, leveraging the information provided by the customer for the registration of a SIM (GSMA, 2018).

Figure 2. Countries in Africa where MTN mobile money is offered

Source: MTN (2019)

What does the proxy initiative entail?

What is mobile money? MoMo is an electronic wallet service that allows users to store, send and receive money using their mobile phones. Each mobile money user has a unique account number, which is the same as their phone number. Customers can access the

services offered by MoMo by dialling the USSD code that is specific to their jurisdiction. The USSD interface is available on basic mobile handsets.

The services offered to MoMo customers include P2P, B2P and P2B payments, which may be in the form of remittances, salaries, loan disbursements and bill payments to name a few. Additionally, customers can deposit into and withdraw cash from their MoMo account by going to a network of MoMo transactional agents. Customers can sign up for MoMo without an existing bank account.

The foundational identity is a nation's proof of identity. The foundational ID for MoMo accounts is the nation's ID number, and the customer presents this identification to satisfy KYC requirements. The core identifier of MoMo is a customer's MTN mobile phone number. Secondary identifiers may include the customer's name and surname.

Customer journey

Individual customer registration. KYC identification requirements are mandatory for SIM registration. When customers purchase an MTN SIM, they need to provide proof of identity and proof of address. Only 40% of all African countries mandating SIM registration have a privacy and/or data protection framework in place (GSMA, 2018). To open a mobile money account, customers also need to provide proof of identity, as all financial services providers (FSPs), including mobile money providers like MTN, must comply with KYC requirements and follow best practice. This ensures that there is commercial reliability of financial services and compliance with financial regulators' rules on KYC. The combination of an active MTN SIM and proven identity enables a customer to register for a mobile money account. Due to the generally relaxed KYC requirements for MoMo accounts, the customer normally has lower transactional limits applied to their MoMo account.

Business customer registration. KYC requirements are also mandatory for business MoMo registrations, but they are more stringent. Businesses may be required to provide business registration documents as part of their KYC compliance before they can open a MoMo account.

Making a payment using MoMo. To make a P2P payment using MoMo, the customer will use USSD codes specific to their jurisdiction to initiate the payment by selecting the payment option in the MoMo USSD menu. The customer will be prompted to enter the receiver's MoMo account number, which is also the receiver's mobile phone number. Once the number has been entered, the customer will be shown the receiver's name to confirm that the receiver details are correct. Once the receiver's information is confirmed, the customer will enter their PIN to confirm the payment. The payment will be processed immediately and both customer and the receiver will receive notification of the payment.

Mistaken payments. If a customer needs to apply for a money transfer reversal, they may do so within a specified time period. The application may be reviewed and where the amount is fully available, the customer will be reimbursed.

Deployment process

Different mobile money models. Mobile money may be deployed in different ways, which include the following models:

- **Bank-led model**. Mobile money operators are directed to partner with a bank for MoMo deployment. This means that the unrelaxed regulatory requirements applied to banks must be adhered to by the MNO partnering with the bank (Mondato, 2018).
- **Mobile Network Operator (MNO)-led model**. MNO's are not held to the same regulatory requirements as banks when servicing deposit or deposit-related functions, and therefore the MNO-led model is more dynamic due to relaxed regulatory requirements (Mondato, 2018).

The model selected for a jurisdiction is dependent on the financial regulatory environment of each country. In some jurisdictions, mobile money implementation comes with mandated mobile money interoperability with other mobile money providers in that country.

MTN and commercial bank engagement. The delivery of MTN MoMo is enabled by a joint venture between MTN and the banks in a country. MTN uses the credit system rather than an e-currency or commodity equivalent of the cash value (Williams, 2013). In setting up to deploy MoMo, MTN must open a trust account[13] with a supervised financial institution in the country they are functioning in. The balance of the trust account must always be equal to the total outstanding (unclaimed) balance of all holders of e-money under the MoMo service. Some jurisdictions may impose capital requirements for MoMo deployment. MTN recruits and trains agents for successful deployment of MoMo. The agents are trained to ensure adherence to KYC requirements for customer registration and transactions.

Regulatory engagement. After completing these steps, MTN must apply for a licence and engage with the mobile money regulator of the specific country that they are looking to operate in. The engagement will be driven by whether the country already has mobile money regulation in place or not. Upon successful engagement with the regulators, MTN gains custody of customer funds. (GSMA, 2018).

Measurements of success

MoMo relatively successful in Africa. MTN has approximately 27 million active and unique mobile money customers in the 14 countries of their operation. MTN has 376 000 active agents and on average50 000 loans issued daily through MoMo. Furthermore, MoMo has enabled USD250 million in inbound remittances and USD400 million in outbound remittances. 3 million customers are now saving an average of USD3 a month (MTN, 2019).

Key themes

Accessibility of MoMo

High mobile phone penetration. There was a 75% SIM connection penetration rate at the end of 2017 (GSMA, 2018), and unique mobile subscriber penetration in Sub-Saharan Africa stood at 45% at the end of 2018 (GSMA, 2019). Some users share phones with different SIM cards and others share both phones and SIM cards.

Limitations to MoMo accessibility. The proof of identity requirements for both SIM registration and KYC contexts raise a concern that they may deny some segments of the population access to basic mobile communications and mobile money services where individuals lack a form of acceptable identification. 48% of adults in sub-Saharan Africa do not have official proof of identity (Cooper, et al., 2018).

Furthermore, access to MoMo may be limited by the following:

- **Mobile connectivity**. Transactions on MoMo are conducted over USSD channels and therefore rely on good mobile network connectivity.
- **High transaction costs**. The increasing transaction costs for MoMo may be exclusionary. These may be impacted by jurisdictions implementing a taxation on MoMo as is the case in Uganda (UNCDF, 2018).
- **Agent network distribution**. If MTN's agent network distribution does not reach individuals in very rural areas, this may be exclusionary as they may not have access to the MoMo service.

Verifiability of MoMo

Second medium verification is possible. At MoMo registration, a customer's ID is verified by agents who have been trained to ensure that ID documents are not counterfeits. Furthermore, MTN may verify a customer's identity through the SIM registration database in the country they are operating in. The SIM registration process and MoMo registration process both require a verified ID (Foundation ID) and therefore the linking of the SIM and MoMo data effectively verifies the mobile number to a foundation ID.

USSD codes and payments. When customers make payments, they dial the USSD code that is specific to their country. The customer verifies payments by entering their PIN before confirmation. The PIN effectively links and verifies the sending number and SIM with the sending foundation ID and confirms the payment.

Trustworthiness of MoMo

Uniqueness

Consistency in mobile number ownership. In most economies, people keep the same mobile phone number for a long time. A customer may only have one MoMo account and this also helps maintain uniqueness of the MoMo account. Each mobile number is unique and registered to its owner upon purchase due to regulation that mandates SIM registration. This makes stealing identity hard. Due to the MoMo verification process, customers may not register for MoMo whilst using a SIM that is not registered in their name upon purchase.

[13] A trust account is a bank account held by a licensed financial institution for and on behalf of the participants in the mobile money service who have deposited cash in exchange for e-money.

Privacy

MoMo facilitates privacy. Registration for MoMo is voluntary and customers only share their mobile number for payments as their mobile number is also their account number. Payments made via MoMo are authenticated by the customer by verifying the receiver's name and entering their PIN, this mitigates against identity theft.

Privacy undermined. In some developing economies mobile phone-sharing undermines privacy, as it allows others to potentially access to private transactional/financial information. However, as mobile phone ownership is on the rise in these countries, this may not be a persistent or significant problem in the future.

Customer experience

Positive impact for the customer. The use of MoMo has become more popular over the years because it is user-friendly and enables the customers to have more secure storage of their money, instead of using cash. People are generally used to using their phones in everyday life, which means using MoMo can be easily assimilated into their everyday lives.

USSD codes. The use of USSD codes for MoMo makes the service very user-friendly, especially for customers in rural areas with very little digital literacy. USSD codes provide a simple menu with easy navigation and limited options for the customer. USSD was originally found on feature phones and was then included on smartphones as residual technology to be retrospectively inter-operable.

Case study 2: TIPS mobile proxy

Context

EU banking context and its regional RTGS. TARGET2 is the real-time gross settlement (RTGS) system for the EU. It processes monetary policy operations, bank-to-bank transfers and commercial transfers. Every five days, TARGET2 processes a value close to the entire EU GDP (European central bank, 2019). More than 1,000 banks use TARGET2 to initiate transactions in euro, either on their own behalf or on behalf of their customers.

What does the proxy initiative entail?

What is TIPS? Target Instant Payment Settlement Service (TIPS) is a real-time retail payments mechanism established by the European Central Bank in November 2018. TIPS offers final and irrevocable settlement of instant payments in euro, at any time of day and on any day of the year. Settlement on TIPS takes place in central bank currency and using the rails of TARGET2, the regional RTGS. As such, using TIPS requires the institutions to be on the TARGET2 RTGS and to additionally be a participant in TIPS (European Central Bank, 2019).

Standardised Mobile Proxy Look-up service to makes instant payments more convenient. To make it easier to send money via TIPS, TIPS introduced the Standardised Mobile Proxy Lookup Service (MPL) which enables actors to execute payments for a beneficiary identified with a proxy identifier. The MPL service is available to all role-players participating in TIPS. The proxy identifier used currently is the mobile number. Consumers can enter the mobile number of the target recipient instead of the bank account details to make payments to them. MPL may be open in the future to implement other types of proxies such as email address, social network ID and business ID (European Central Bank, 2018).

European bank account serves as foundational ID. Proxy identifiers are linked to the underlying European International Bank Account Number (IBAN). IBAN serves as the foundational identity on which all KYC documentation is based. As such, the robustness of the IBAN is dependent on the robustness of the KYC process at that bank.

Second order verification of mobile number possible. A particular aspect of mobile proxies is that they have to be identified by their Mobile Station International Subscriber Directory Number (MSISDN). Each phone number may be linked to one and only one IBAN at any given point in time, whereas each IBAN may be linked to either one or multiple phone numbers at any given point in time. If an individual has multiple accounts, each of them should be linked to a different mobile number.

Data mapped into one place for ease of use. The Mobile Proxy Look-Up service, MPL, relies on a central repository. The central repository relies on a Proxy-IBAN Mapping Table. This includes all correspondence established by each MPL Actor between proxies and IBANs. Each element of the mapping table will include the following attributes:

- Proxy (e.g. mobile number)
- IBAN

- Account Owner (name of the account owner, optional)
- Registration Timestamp (timestamp of creation of last update)
- MPL Actor BIC (BIC of the TIPS Participant or Reachable Party)
- Valid From Date and Time
- Valid To Date and Time

Customer journey

Both sending and receiving customers must be enrolled on TIPS MPL to use the service. The customer downloads the bank app. The customer can then link a phone number or email address to their account. This registers the user on the MPL system. Once registered, the user can send money to another user that is enrolled on the MPL system. The user can then send money instantly to the beneficiary by sending to the proxy ID (Banks of Spain, 2019).

Look-up service links proxy IDs to underlying IBAN and BIC. **Error! Reference source not found.** describes the technical process of sending money via the TIPS MPL. Initially, the originator sends a request to the originator PSP to initiative a payment. The originator Payment Service Provider (PSP) then submits a look-up request to the MPL which responds with confirmation for the underlying IBAN identity of the beneficiary and the relevant BIC. The originator PSP then instructs TIPS to make a payment to the beneficiary using IBAN and BIC. This results in an instant payment that the consumer can make by simply knowing the proxy identifier.

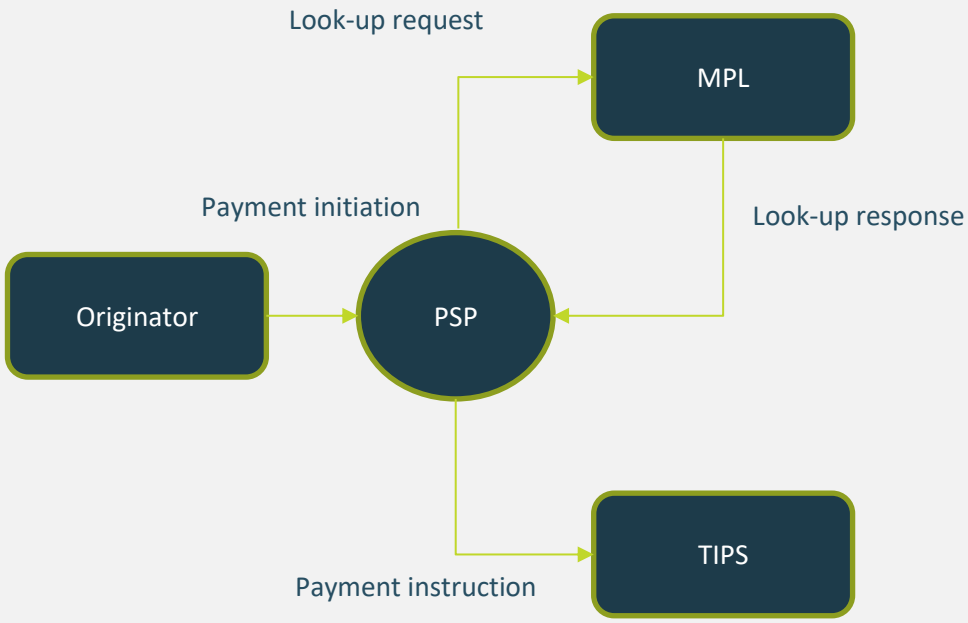

Figure 3. TIPS MLP payment process

Source: European Central Bank (2019)

Deployment process

TIPS adheres to the same participation rules valid for TARGET2. There are three ways to access TIPS (European Central Bank, 2019):

- Participant – eligible to open one or more accounts in TIPS
- Reachable party – able to access a participant's TIPS account by entering into a contractual agreement with that participant
- Instructing party – enters into a contractual agreement with one or more participant/reachable party/parties to instruct on their behalf

Lack of adoption of the MPL systems undermining its usefulness. The TIPS system comes after several European countries have already launched their own rapid payments system, creating a fragmented space. In addition, despite being participants in the system, some banks do not offer the option of using the telephone number as a proxy and still require the sender to provide the IBAN of the receiver. This undermines the concept of facilitating the use of ID proxies.

Cost per transaction kept low for the first two years of deployment. To participate in TIPS, service providers must set aside part of their liquidity on a dedicated central bank account which is used for dedicated instant payments. The scope and reachability of TIPS is then determined by the number of participants and reachable third parties. Participants (banks) are charged 0.2 EUR per transaction for at least the first two years (Bayle de Jesse, 2017). It is then up to the bank to decide how much they charge their customer per TIPS transactions (Pires, 2019). In addition, the first 10 million payments made by each TIPS participant before the end of 2019 are free of charge. TIPS operate on a full cost recovery and not-for-profit basis (European Central Bank, 2019).

TIPS competing with other instant payment services. Currently, there is no interoperability with other instant payment schemes that have been developed for the region or for specific EU countries. For example, The European P2P Mobile Payments mechanism (SEPA proxy lookup service) is not interoperable with TIPS. In addition, country schemes like Instapay in Holland are not interoperable with TIPS. TIPS is therefore competing with other instant pay services that participants and users are possibly more familiar with.

Measures of success

Limited participation in TIPS undermining success. As of April 2019, only 30 banks are participating in TIPS, mostly from Spain and Germany (Buck, 2019). This is because participation in TIPS is completely voluntary, and many banks have simply decided not to participate. The European Commission is therefore pondering a "regulatory push" to encourage adoption of the new TIPS instant payments service and make it a genuine rival to the card schemes and tech digital wallets. Since the TIPS systems has not yet been widely adopted, the MPL systems is hardly utilised.

Key themes

Accessibility of TIPS

TIPS is highly accessible and expected to improve the payments environment for business. Mobile phones and the internet are ubiquitous in Europe, which makes the phone number a very accessible proxy. In the case of Europe, access to banking is already very high, so the focus of TIPS MPL is more about making payments easier and more efficient than to enlarge their customer base. In particular, TIPS is expected to improve the ability of fintechs and other start-ups to make regional instant payments. Previously, they would have to go through their banks at some point, but with a standardised system across all banks, fintechs will benefit from faster and cheaper payments (Pires, 2019).

Lack of integration into banking apps limits accessibility. Without effective integration of TIPS and TIPS MPL into the banking payments apps, the service is unlikely to be accessible to users. In some cases, banks have not adopted TIPS yet, while in other cases it has been adopted but not implemented in a user-friendly way.. As such, users find it difficult to engage with or to understand. This is troubling as users are more likely to use services that they do understand and can easily access.

Verifiability of TIPS

Second medium verification possible. As discussed above, the customer identity linked to the mobile number is verifiable against the MTO routing back-end system or third-party databases. The mobile number proxy is compatible with SMS, USSD, voice (alone or with a thin SIM), API communications or validation systems. In addition, mobile phone numbers are identified by their MSISDNs (Mobile Station International Subscriber Directory Numbers)[14].

IBAN linked to additional foundational identity. In addition, the underlying IBAN number is linked to the user's national identity card or other foundational identity. IBANs are subject to KYC requirements under EU regulation. These differ depending on the jurisdiction, but ultimately serve to verify the identity of the IBAN.

Trustworthiness of TIPS

Uniqueness

Mobile phone a unique identifier. In Europe, people keep the same phone number for a long time, even after changing the phone device many times. Moreover, phone devices and phone numbers are rarely shared. Those attributes, in addition to the verification of phone numbers via MSISDN make mobile phone numbers a unique identifier.

Privacy

Facilitates privacy of account details. The use of a mobile number as an ID proxy shields the underlying account details. As discussed under verifiability, the mobile number may be underpinned by another proxy to ensure robustness, whilst still maintaining accessibility at the front end.

Compliance with regional regulations and standards ensure protection of data. The scheme observes strict data management, integrity, confidentiality, and protection requirements, as enforced by *GDPR*. (General Data Protection Regulation). MPL complies with the Market Infrastructure Security requirements and controls and with the Market Infrastructure Cyber-resilience requirements (MISRC).

Customer experience

Customer experience hampered by slow implementation. Mobile phone numbers are more readily at hand than bank account numbers, since most people would have the phone numbers of their contacts saved on their phones. This makes it much easier and more convenient for consumers to make payments. However, lack of adoption of TIPS across all banks and lack of customer awareness is hampering adoption.

Voluntary participation and usage of ID proxy ruining the customer experience. Although the TIPS service makes payments more convenient for consumers, very few banks have adopted it, so the option is not available to everyone. Furthermore, even where TIPS is available, some banks do not offer the option to use the phone number as a proxy which results in a poor customer experience. In addition, the final cost for customers depends on each institution, and many cases, immediate payments are costly.

[14] MSISDN is a number uniquely identifying a subscription in a Global System for Mobile communications or a Universal Mobile Telecommunications System mobile network. It is the mapping of the telephone number to the subscriber identity module on a mobile or cellular phone.

Case study 3: Mexico Interbank Electronic Payment system (SPEI)

Context

The Mexican context. Mexico has a population of nearly 13 million and a GDP per capita of USD8,910. Nearly 65% of the Mexican population possessed an account at a financial institution in 2017. In the same year, 32% of adults reportedly made or received a digital payment according to the 2017 World Bank Global Findex (2018). This represents as an increase from 29% of the population in 2014.

What does the proxy initiative entail?

What is SPEI? SPEI was established in 2004 and is a near-real-time, instantaneous, electronic funds transfer system that is owned and operated by Banco de México (henceforth referred to as Banxico). It was designed to settle large volumes of payments in real time and has since evolved to settle both small and large values. SPEI currently accommodates at least 15 payment types that range from paying school fees, paying gym membership fee to repaying loans. These payments can be made 24 hours a day, seven days a week, 365 a year since 2016, and are only accessible through internet or mobile banking.

The foundational ID for SPEI. The core identifiers of all participants in the SPEI system are the name and the Personal ID code[15], or alternatively the Federal Tax Registry number. Financial institutions must collect these data from customers to authorise using SPEI. To these core identifiers, there are several beneficiary ID proxies to choose from when ordering a payment via SPEI:

- Standardised Bank Code (CLABE). This is a unique 18-digit code that the bank assigns to every account. A customer will have as many CLABE codes as accounts in the financial system.
- Card PAN number (debit card number [16 digits]); or a
- Mobile phone number (cellphone number [10 digits]). The same mobile phone number can be linked only to one account for each bank, i.e. the same mobile phone number can be linked to several accounts in different banks, but only to one account for each institution.

Since SPEI payments are always made between accounts at different banks, the linking of the above identifiers to the base identifier (account number) is crucial.

Customer journey

Enrolment

Non-homogenous bank linking procedure. A customer can link a phone number to a bank account at a bank branch or remotely via internet or mobile banking. Each bank determines its own linking procedure. However, when a client requests the linking process

[15] In Spanish, Clave Única de registro poblacional (CURP). It is a unique identity code for both citizens and residents of Mexico.

via a mobile device, the request must be made from the number that is going to be linked. Identifiers are stored on the SPEI, which is a centralised and computerised infrastructure.

Usage

First-time usage of SPEI. Every time an individual wants to send money to a person or company for the first time, (s)he will have to register the account prior to being able to make the transaction. After registering the receiving account (including information on the name, valid ID proxy, recipient bank and max amount that can be sent to this account), there will be a latent time before the customer can make the payment[16]. Mobile banking users are exempted from this rule for very low-value transactions[17].

Making an SPEI rapid payment. The customer can log in to their banking app or online website, introducing their credentials. The customer can choose to make a rapid payment, and this is the way SPEI is commonly referred to customers. The customer will select the account and will input the amount and the concept or reference number for the transaction. The bank will prompt a confirmation screen with a summary of the data input and will require an additional authentication method. The authentication method will vary depending on the bank and can comprise a password, an OTP, a token, etc. Transactions below 8,000 pesos can be exempted from this rule.

Completing the transaction. Once the transaction is validated, the customer receives a payment receipt message with a reference number that could be used at any time for monitoring the payment and for claiming purposes in case of error. The receipt also provides the series number of the security certificate, the originating chain of events, and a digital seal that allows validation of authenticity.

Deployment process

Banxico promoted SPEI. The SPEI system became operational in August 2004 and gradually replaced its predecessor, the Extended-use Electronic Payments System (known by its Spanish acronym, SPEUA), which ceased operations in August 2005. The set-up and evolution of SPEI is a clear example of a highly engaged central bank and its core role in promoting the service[18]. In addition to regulating, supervising and managing the SPEI, Banxico has launched numerous awareness-raising campaigns to educate customers and increase adoption.

Ubiquity increased by a gradual roll-out. At the start of SPEI's operations in 2004, only banks were allowed to participate in the system. However, Banco de México has allowed non-bank financial institutions to participate in it since 2006[19], increasing the ubiquity of SPEI. Banxico owns the SPEI and developed a set of rules for all participants. Banxico monitors and enforces compliance with the rules. Institutions participating in SPEI must enter into a contract with Banco de México to define their rights and obligations regarding the provision of services related to this system.

[16] Latent time can be of a couple of hours before the service is available
[17] Transactions under 250 UDIs made via mobile banking are exempted from registering the receiving account prior to making the transaction. Peso-UDI conversion was 6.2 in January 2018.
[18] http://www.cgap.org/sites/default/files/Interoperability_in_Electronic_Payments.pdf
[19] Banco de México's Policies and Functions Regarding Financial Market Infrastructures, Banxico 2016

Cybersecurity response to hack attack. After a hack attack to the SPEI system in 2018, Banxico reinforced its rules and protocols, specially concerning cybersecurity rules all participants have to follow. Initially, Banxico did not require banks to follow specific cybersecurity norms. It is perceived that stakeholder involvement is uneven. SPEI's governance would benefit from a formal participants' consultation mechanism; among other objectives, this body would ensure access to the FMI decision-making by all participants on an equal footing (World Bank 2016).

Measurements of success

SPEI relatively successful. In 2015, SPEI-processed transactions for the equivalent of 10 times the country's GDP[20]. According to Banxico, low-value payments made via SPEI on average grew by 32% annually between 2010 and 2017. The average transaction amount decreased from 3,000 to 1,950 pesos. In 2017, 1.3 million transactions were performed on average every day. Peak days reached up to 7 million transactions via SPEI. Standardisation of account numbers has also helped to reduce rejection rates, thus improving trust in the system.

Key themes

Accessibility of SPEI

Internet required for SPEI access. The customer needs a smartphone or computer to be able to make a rapid payment. This represents a mild barrier, since smartphone penetration in Mexico was 74% in 2018, though only 42% of Mexican used computers by the same time. The customer's need to access internet and online banking usually also has a cost (monthly fee or other) in Mexico. Both the cost of data and the cost of online banking may represent a barrier to low-income people and hamper adoption[21].

Tiered bank account system for increased access. Mexico has a tiered system approach with different account levels with different deposit limits. All types of accounts, including the more restrictive ones, have an assigned CLABE code, which is one of the valid ID proxies used in SPEI. Difficulty obtaining KYC documentation required to open a mobile bank account and inconsistent acceptance of different types of KYC documentation to open mobile bank accounts (Faz, 2013).

Verifiability of SPEI

Customers can track their payments. When a payment is made, customers can verify the SPEI connection statistics to identify whether one of the banks involved experienced a connection problem. If a customer can verify a connection failure, then they will have to attempt to process the payment again (Banco de Mexico, 2019).

[20] http://documents.worldbank.org/curated/en/735661507876121410/text/120395-WP-P159016-PUBLIC-Financial-Sector-Assessment-Program-series-Mexico-2016-FSAP-Update-DAR-PFMI-SPEI.txt

[21] Mexico is tied with SA at 51st place on 2018 Inclusive Internet index.

Trustworthiness of SPEI

Uniqueness

CLABE code and beneficiary name maintain uniqueness. The standardisation of bank account numbers (CLABE code) has helped to reduce rejection rates thus improving trust in the system. The sender must input one of the accepted ID proxies (CLABE code, card code, or phone number), as well as the name of the recipient. However, the name of the recipient is not verified by the financial institution. The confirmation message the bank prompts before a customer validates a transaction only includes the beneficiary name as the sender input it. This practice suggests there is no underlying verification between the ID proxy and the name of the recipient.

Potential for fraud with CLABE only usage. In 2015, the Mexican OMBUDSMAN warned customers of detected fraud cases where individuals were provided with a fake Standard Bank Code that did not belong to the company it supposedly did. This resulted in customers sending money to unintended accounts, and the OMBUDSMAN declining responsibilities on behalf of the financial system, as the only valid identifier was the CLABE/Standard code one[22].

Privacy

Layered validation. Since authentication is needed for both log in into mobile or internet banking and for validating the transaction, there is little risk that a third party can make a fraudulent use of an account, even in the case of theft of mobile phone. Proxies are embedded within the national RTGS that's been stress-tested against: a failure in the main technological infrastructure of SPEI; the impossibility of access to Banco de Mexico's facilities; connection and communication problems, both of a single participant or of SPEI itself with all the participants.

Vulnerability to attacks undermines trust in the system. Hack attacks in 2018 proved nevertheless that systems are not immune. In this particular case, the vulnerability seemed to be within the bank's systems and policies. Further enforcement of the security rules was implemented to avoid this risk in the future, as it highly undermines trust. The confirmation receipt generated after a transaction is sent by the sending bank with its digital signature as a validation that the information contained therein were generated by the payee's institution and that the related transaction is authentic.

Mobile phones shared between family and friends may allow for financial information of sender being leaked. Additionally, it is worth noting the vulnerability of mobile phone numbers to cyber-attack.

Customer experience

Customer experience varies with each bank. Each bank developed its own interface, although some rules had to be complied with in terms of fields required, information provided to clients, etc. This may have led to some differences in the customer experience.

SPEI is more user-friendly. Including phone number as ID proxy makes the system more user-friendly as compared to CLABE codes and card codes. In addition, being able to register one phone number on multiple accounts – at different banks – represents an important advantage, as many people may only have one phone line. On the downside, having to register a receiving account and experiencing latent time before being able to make a payment may represent a significant pain point and may hamper usage.

[22] https://www.gob.mx/condusef/prensa/alerta-condusef-por-modalidad-de-fraude-en-la-venta-de-vehiculos

2.2. Email address

Key advantage:

- User-friendly and more convenient to provide than bank account details

Key disadvantage:

- Risks high levels of exclusion among those of the population without access to an email address

What does the proxy entail?

Email address as main identifier. An ID proxy that is based on an email address uses an individual's email address as the main identifier of the receiver of a payment, instead of the individual's bank account or electronic wallet number. To register for an email address ID proxy service, a client would usually need to register their email address either with a financial institution, government agency and/or an online platform that facilitates payments. They may be asked to provide additional information such as their name, address and mobile phone number to add a second layer of identification. In the case of an online payment platform, such as PayPal, clients may need to add and verify a checking account or credit card as the underlying instrument activated via the email ID proxy.

How accessible is it?

Multiple proxies possible per individual. It is easy for an individual to open different email accounts using the same or different servers. Each of these email addresses could eventually be used as a distinct ID proxy linked to an account. Our assumption is that this situation may be particularly applicable to the segment of the population which already forms the customer base of banks in South Africa.

Dependent on internet penetration. Most developed economies have high internet coverage infrastructure and high internet penetration. This facilitates the use of email address proxies. In South Africa, the number of active internet users is estimated at 31.2 million people (Statista, 2019), which represents approximately 86% of the adult population (StatsSA, 2018). According to ICASA, the total number of fixed broadband subscriptions increased from 3 million in 2017 to 7.4 million in 2018. In many developing economies, however, internet coverage remains relatively low (ICASA, 2019).

Facilitated by growth in smart phone penetration. Most developed economies also have high smartphone penetration, thereby facilitating easier, continuous email access. This is the case in South Africa: ICASA estimates smartphone penetration at 80% of the population as of September 2018[23]. Again, smartphone penetration lags in developing countries, which undermines the accessibility of email as an identity proxy.

Email losing traction as main communication tool. The booming of social media may have rendered email obsolete for some people, especially for younger people and for those segments of the population who leapfrogged accessing internet from a computer to directly connecting from a smartphone. Despite this statement, email penetration and usage in

[23] This estimate is higher than some other sources. The 2018 WeAreDigital report for South Africa suggests a 60% penetration rate. Either way, it is clear that the majority of South African adults now have smartphone access.

countries such as the USA continue to grow. Further interrogation of demand-side research is needed to ascertain what the case is for South Africa.

***May be undermined by high data costs*.** In most developing countries, mobile data costs are high, therefore some individuals may not have access to or be able to regularly use an email address. In South Africa, data is relatively expensive, ranking 35th out of 50 in Africa, with an average 1GB prepaid mobile data charge of USD7.84 (Raul, 2019).

Requires digital literacy. Furthermore, limited digital literacy, which is the case in many developing countries can be a barrier to using an email address as an ID proxy.

Is it verifiable?

Standard procedure for email address verification. The client would typically be required to verify their e-mail address through their institution-specific verification process. This verification process may involve entering a verification/confirmation code that is sent to the email address. An alternative method could include processing a micropayment, where the client will enter the micropayment details to verify the email address and the linked bank account.

Limitations to second medium verification. There is, however, no underlying database of email addresses linked to an identity data registry that could be used for second-step verification of the underlying identity of the user (as would be the case for mobile numbers via SIM card registration). This makes the email address proxy less verifiable than some other proxies.

How trustworthy is it?

Uniqueness

Each email address is designed and registered as unique through providers such as Google or Yahoo for example. However, at least three factors undermine the uniqueness of email addresses as an identity proxy:

- ***No clear link to underlying identity***. An individual can easily open an email account using the name of another person or well-known institution, creating confusion about the real identity behind the ID proxy[24]. Email addresses may also be very similar among different people. In some cases, the difference may be just a letter or the email extension/server. This may lead to false positives, as a person may feel confident that they are sending money to someone who may not be the real owner of the account. This situation can be mitigated by providing additional details of the account holder such as the full name, so the sender can verify the identity of the receiving party.
- ***Potential privacy concerns***. This proxy can represent a privacy concern and safeguards should be in place to avoid high frequency proxy database queries from one or more grouped senders, particularly without resulting transactions. Where possible, audit logs of proxy queries should be maintained and monitored for abuse.

[24] For example, an account called SARB@gmail.com

Privacy

Generally private. In most developed economies, email addresses are individual and rarely shared, which makes an email address a sufficiently private ID proxy. To increase the security of the ID proxy, email can be coupled with other ID proxies such as mobile telephone number (as applied by PayPal). This helps users monitor access on their account and reset their password in case of password loss.

May be undermined by email address sharing. Should more than one person share the same email address (for example within a family), privacy is undermined. This may discourage those, who wish their financial transactions to remain private, from using this eservice. However, email address sharing is probably less prevalent than sharing of phones or SIM cards[25].

Susceptible to cyberattack. A more significant privacy concern is that email addresses are vulnerable to hacking and/or other cyberattacks. Email travels across public networks and if either the email or the content is not encrypted, they can be readily accessed employing telco to telco backend communication channels, including SIM swaps and OTP interception.

Customer experience

User friendly. An email address is a convenient identifier for consumers, as it is easier to remember than an account number.

Potential friction points. If an individual ceases to use an email account, he/she may need to change the ID proxy stored within the system. This can erode the user-friendly nature of the process, which the consumer may find inconvenient. However, given the fact that most people use the same email address from the major providers over time, this scenario does not seem probable. The customer experience may also be undermined where an individual loses the password to his/her email account, which may prevent account access. Email servers usually offer recovery methods, which again makes this scenario less probable.

[25] Demand-side research is required to ascertain the extent to which email address sharing creates privacy concerns.

Case study 4: Google Pay (GPay)

What does the proxy initiative entail?

Recouping all Google payment services into one platform. Google Pay (GPay) is a payment processing and digital wallet platform created by technology company Google. It can be accessed through a mobile app and online website using most phones and some watches running on Android operating systems. It may also be accessed via Chrome, Safari or Firefox browsers. In 2018, GPay replaced all previous Google Payment products, such as the previous Android Pay launched in 2015, Google wallet apps and previous Google Pay and Google Pay Send (Google Pay, 2019)

Linking the Google account with a payment method. To use GPay, an individual has to link card information like credit, debit and loyalty cards with their Google account. In the UK and US, Google also accepts linking a bank account to a google account. GPay can also link to an individual's PayPal and Visa checkout accounts for purchases in selected countries at participating stores. An individual can link multiple cards and bank accounts to the same Google account.

Sensitive payment data is highly secure on the GPay platform. Once a GPay user has added a credit or debit card to their Google account, GPay then requests a token to represent the card from the bank that issued that card. Once the token is issued, this card is now "tokenised," meaning it has a unique and random identification number associated with it. GPay then encrypts the newly tokenised card and stores this information in its database (Betters, 2018). When a customer is making an online payment or paying in a store, GPay responds with the customer tokenised card and a cryptogram which acts as a one-time password. The card network validates the cryptogram and matches the token with the customer's actual card number.

Once payment methods are established, GPay can be used to make payments in various ways:

- **Online payments.** Purchasing of goods or services online.
- **In-app purchases.** Purchases made within the GPay application
- **Retail purchases**. Purchases made in physical stores. Retail purchases use NFC technology, which is currently accepted in 29 countries.
- **P2P money transfers**. An individual can keep a balance on their google account or make transfers directly from his/her bank account, with certain limitations on the amounts[26].
  - This functionality is currently operational only in the US and UK, and GooglePay has recently announced the service will no longer be available in the UK from September 2019 (Li, 2019). This movement follows Facebook's removal of similar capabilities from European markets, earlier this year.

Proxy identifiers make it convenient to use GPay. Each of these use cases uses a different proxy. P2P money transfers use the Google email address or phone number as the ID proxy. The person can make transfers to any email or phone number, regardless of the

operating system used by the receiver, or whether the receiver has a GPay account or not. Retail purchases are done using NFC. Customers need to have an NFC enabled android Smartphone and will be able to pay at stores with an NFC reader. GPay supports EMV contactless or MSD (Magstripe) contactless payments if EMV contactless is not available. POS devices should be compliant with the ISO 14443 standard (Google, 2019).

Google accounts serve as robust foundational IDs. Google is able to cross-correlate information such as GPS information on Android phones, browser usage patterns, IMEI data, SIM data, keystroke patterns, voice, and computer IP address. Cross-correlating this kind of information allows Google to create a detailed digital identity for a consumer, even if that consumer has multiple Gmail accounts, bank accounts and phone numbers. The Google account is therefore the robust digital foundational identity upon which proxy identifiers, such as bank accounts, phone numbers and email addresses are based.

Customer journey

***Name, email and phone number as proxy indicators for identity*.** To use GPay, an individual has to download the app on their Android smartphone or connect to GPay through a computer. Consumers must then set up a profile using either of these platforms. The profile includes a number of indicators such as phone number, name and email address. The bank account or card of the person serves as the *foundational ID* while the *name, email or phone number* serve as proxy IDs.

Verification a precursor to acceptance of payment information. To get started, the person must register at least one method of payment as described above. The person would then receive a confirmation code from their bank to verify bank ownership. Once the card or bank account is verified, the person can start making online transactions, at stores and P2P. If several accounts or cards are registered, the person needs to select the default card or account from which payments will be made.

Payments are made differently depending on the use case:

P2P transfers. To make a transfer, an individual can select any of their Gmail or Android contacts. Alternatively, they can type in any new email or phone number. If the recipient does not have a Google account, Google will automatically create one and will later ask the receiver to complete the opening to receive the funds. If the receiver does not complete opening the account in 14 days, the money is reversed to the original sender. The receiver does not need to have a bank account if the value is below USD2,500. A GooglePay user can also request an amount from any Gmail contact. The money is automatically transferred into that person's listed bank account, if the request is accepted (Google, 2019).

Online purchases. If an online application or website accepts GPay, there will be the option to "Pay with GPay"#", when conducting the transaction. The user has to simply click on the relevant button to make a payment via GPay.

[26] There are limits on the amount that can be transferred. Single transaction: Up to USD10,000/ In 7 days: Up to USD10,000/ Florida residents: Up to USD3,000 every 24 hours. For transactions over USD2,500: The recipient will need to add a bank account to claim the money.

Retail purchases. To make purchases in physical stores, the user has to unlock the Android Smartphone and then connect it to the relevant NFC-capable POS machine. There is no need to open the app to make the payment, as this is done automatically when the phone nears the POS device. There is no additional authentication needed to confirm the payment (Google, 2018).

Additional features improve security and utility. GPay app will show the most recent purchases on the home screen. Users can also check which stores nearby accept GooglePay; this is shown via Google maps. If a person loses their phone, Google allows the user to remotely wipe the device and remove all card details. Payments normally require online access, though a number of transactions in store can be conducted offline if there is no connectivity.

Key themes

Accessibility of GPay

Retail payments are convenient but dependent on technology. From a customer perspective, the requirement to have a smartphone with NFC technology can be an issue for countries where USSD is predominant, or where consumers are lower income and don't have NFC-enabled phones. Although not particularly new, this type of technology is normally only available on mid to high-end smartphone devices. In addition, the phone needs to be running on Android KitKat 4.4 or higher (Rutnik, 2019). The latest version of Android is not always installed or available on phones with NFC technology (even high-end phones). From a merchant perspective, GPay needs the merchant to have an NFC reader/POS device, and not all terminals are equipped to do so.

*GPay highly accessible but some challenges exist for developing countries***.** For P2P and online payments, GPay is highly accessible as you can create a GPay account by downloading the app, and you can also connect via several browsers from any computer. The options of using email addresses and phone number means the ID proxies are almost ubiquitous as everyone has at least a phone number. Moreover, being able to send money to someone without a GPay or bank account further increases accessibility. For P2P transfers, only users in the US can benefit from this feature, but this is likely to expand as the service develops. The only drawback from the perspective of a developing country is that GPay needs internet access and connectivity. This can become an accessibility barrier in countries with low penetration of Internet, low Smartphone penetration or high cost of data.

Verifiability of GPay

In-person verification. In retail purchases, it is easy for a sender to verify that they are transferring the money to the right receiver, as the payment is done in close proximity and the individual can do the verification in-person. In addition, the person making the payment via GPay can verify their identity by unlocking the phone (either biometrically or using a PIN code). There are some concerns that payments do not require biometric authentication, as is the case for similar services such as Samsung Pay and Apple Pay. This means that the authentication of the sender may be less secure.

Standard procedure for email address verification. The client would typically be required to verify their e-mail address through their institution-specific verification process. This verification process may involve entering a verification/confirmation code that is sent to the email address.

Limitations to second medium verification. There is, however, no underlying database of email addresses linked to an identity data registry that could be used for second-step verification of the underlying identity of the user, as would be the case for mobile numbers via SIM card registration. Although the user provides a number of additional identifiers during sign up for Google services, the accuracy of these is not verified against another database.

Google digital identity serves as second-step verification. The robust Google identity that is established through cross-correlations, as discussed above, is able to provide second-order verification and detect fraudulent activity. For example, if payments are suddenly made from devices, locations, or platforms that are not typical of the digital identity, Google can pick this up and flag or request additional verification from the Google identity. It also has automatic alerts which notify the Google account of suspicious activity that may have already taken place. In addition, the Google account is linked to the bank account which is itself linked to foundational identifiers like the national identity number. This could also be used to verify identity.

Trustworthiness of GPay

Uniqueness

NFC retail purchases guarantee uniqueness. Every NFC chip has a globally unique, manufacturer supplied and read-only identifier that can be read by most NFC devices. When paying for goods/services using NFC technology, the ID proxy generated for the user is highly unique.

No clear link to underlying identity with email ID proxy. Each email address is designed and registered as unique through providers such as Google or Yahoo, for example. However, some factors undermine the uniqueness of email addresses as an identity proxy. For example, an individual can easily open an email account using the name of another person or well-known institution, creating confusion about the real identity behind the ID proxy[27].

Similarities in ID proxies can lead to false positives. Email addresses may also be very similar among different people. In some cases, the difference may be just a letter or the email extension/server. This may lead to false positives, as a person may be confident that they are sending money to someone, who may in fact not be the real owner of the account. However, since GPay is mostly designed to be used among your known contacts who are already registered in your agenda, this risk should be mitigated.

Privacy

[27] For example, an account called SARB@gmail.com

Highly secure retail payments. NFC payments are dynamically encrypted – the system generates a single-use transaction key that can only be used once and expires within seconds – which makes the transaction highly secure. NFC payment readers also connect to only one NFC payment device, at a time, and can therefore only process one payment at a time. Moreover, due to the short-range communications setup, there is less probability of unknown connections.

Tokenisation and encryption protect sensitive account information. The tokenisation of bank and card details for all payments (online, NFC-enabled retail purchases, or P2P) means sensitive information is not disclosed to merchants or stored in the Google database. In addition to the tokenisation of bank account details, messages that are sent back and forth using the account details are encrypted. This means that bank account details are protected in multiple layers.

No extra security if in the wrong hands. Although the user must first unlock the device, Google requires no additional PIN or password to complete a transaction, which undermines security. As mentioned, however, there is no payment verification process, so if someone knows how to unlock another user's Smartphone, the security of that GPay account may be compromised. The person may be able to make payments on their own behalf in stores, as well as see all their personal information on the Google app.

GPay information is only as secure as a google account. If a google account password is weak, or if the user's computer automatically accesses the google account, privacy and security may be compromised. In cases where phones are stolen, remote wiping of the account details is a feature that increases the privacy and security of the account.

Customer experience

Seamless and quick payments. To complete a transaction, the individual only needs to place the NFC enabled phone/bank card near an NFC reader or NFC-enabled device. No additional action is needed. P2P payments through GPay are also quick and convenient, as the person can quickly select any of their Gmail or phone contacts and even send money to someone who does not have an account. For online payments, GPay spares the user from entering the card details in every transaction, therefore saving time. Allowing payments via the app or via a web browser also facilitates the ubiquity of the system. Allowing to clients to register and pay with multiple cards and bank accounts gives high flexibility to the customer and allows all the payment methods together in one app.

Restrictions in availability of GPay "ready" stores limit us cases. Currently, there are a limited number of online stores that are accepting GPay. In addition, the need for advanced POS devices that are NFC-enabled reduces the availability of NFC-based payments in retail stores. This is of particular concern in developing countries, where access to these technologies are still in their infancy.

Brand changes and country differences create confusion. The continuous change in branding of the service (from Android Pay and Google Wallet to ultimately having one combined GPay) may have created confusion among users. The fact that not all the services are available in the same countries adds to the confusion. However, most similar

services like Apple Pay and Samsung Pay also operate within a specific set of countries[28]. For example, Samsung Pay is only available in one African country (South Africa). Although each customer will most probably use their preferred option and stick to it, the full range of options for sending money (online, in stores, P2P) using different proxies for identifying the receiver may be overwhelming for a beginner.

[28] Samsung Pay is currently available in South Korea, United States, China, Spain, Australia, Singapore, Puerto Rico, Brazil, Russia, Canada, Thailand, Malaysia, India, Sweden, United Arab Emirates, United Kingdom, Switzerland, Taiwan, Hong Kong, Vietnam, Belarus, Mexico, Italy and South Africa (Samsung, 2019).

Case study 5: Australia's PayID

Context

The Australian context. Australia has a high-income economy with a population of approximately 25 million. 100% of Australia's population above 15 years old have an account with a financial institution.

No consistent standard for identity verification. The national identity of Australians consists of various weighted identifiers, based on a risk-based approach. The primary identifiers considered in Australia's national identity include a driver's licence, a photo card[29], birth certificate, citizenship certificate and a passport.

What does the proxy initiative entail?

The launch of the New Payments Platform (NPP). In desiring to facilitate real-time and more customer friendly/ accessible payments, the New Payments Platform (NPP) was launched in February 2018 together with the PayID system. (PayID, 2019). The NPP operates 24/7, 365 days a year, and is an open access platform (Thompson, 2019).

What is PayID? Participants of the NPP can register a customer's bank account to an identifier proxy called a PayID. When payments are made, they can be addressed to the PayID instead of the usual bank account number; though they can still use the latter. PayID may be a phone number (mobile or landline) or an email address for individuals. In the case of businesses and organisations, the identifier can be an Australian Business Number (ABN) or an Organisation ID (PayID, 2019). When an individual has more than one account, he/she will need to link a different email address or phone number to each of the accounts.

Organisation ID for businesses and organisations. An Organisation ID, or OrgID as it is called, is an identifier for businesses and organisations using preferred text. This OrgID was designed for business and organisations because they have multiple sub-accounts for different purposes.

Customer journey

Registering for PayID. For the individual customer, sign up to PayID is completely voluntary and not linked to a central database. A customer can remotely enrol themselves by logging into their bank app or online banking channel. Then, the customer will link his/her account to a phone number or email address[30]. Each bank has its own verification process to ensure that the phone number or email address is belongs to the customer. This is usually done by sending an OTP to the phone number or a code to the email address of the individual. The individual then must input confirmation.

Businesses' and organisations' journey. To create a PayID using an ABN, customers need to link their already registered ABN to an eligible bank account. In the case of Institutions wishing to register an OrgID or preferred name, the representative of the organisation

[29] A Photo Card can be used as photo identification in the absence of a driver's licence. It has the same application process and security features as the driver's licence (https://www.service.nsw.gov.au/transaction/apply-nsw-photo-card).

must go to a bank branch and speak to a consultant to help them register on site. KYC requirements for registering an OrgID are more stringent.

Making a payment using a PayID. When a customer initiates a payment, he/she needs to input the PayID (telephone number, email, ABN or Org ID) of the receiver. Then the system would prompt additional information of the receiver, including full name and account number, so the sender can verify whether the information is correct before validating the transaction.

Deployment process

Deployment of NPP and PayID roll-out

The development of the NPP. The NPP is mutually owned by 13 institutions[31] which conjointly created a third-party company called New Payment Platform Australia (NPPA) in charge of maintaining and developing the platform, under a self-sustainable approach (not profit maximisation approach). The aim of sharing infrastructure was to spur on competition among the Australian financial sectors. NPPA provides the governance structures, and the rules and protocols for all the participating banks to follow. NPPA also has sanctioning power and can introduce penalties when any of the members do not comply with the agreed rules.

Financial institutions that do not own the NPP can participate and connect indirectly to the NPP through Osko, an overlay service that enables real-time payments, built on the NPP. Osko enables fast payments to a PayID or an eligible bank state branch (BSB) and account number combination (Osko, 2019).

Engagement of the Reserve Bank of Australia. The NPP and underlying ID proxy system, PayID, was developed with the support of the Reserve Bank of Australia. Although the NPP is privately owned, the RBA is a shareholder. This increased buy-in and gave legitimacy to the NPP (Stakeholder interview, 2019). There were no specific changes in regulations with regards to the launch of the PayID addressing service.

Simultaneous deployment being key. The PayID system was launched in conjunction with NPP. Launching both simultaneously was key to ensure the success of the initiative (Stakeholder interview, 2019). The PayID service was therefore ready at launch. PayIDs give certainty to payers, avoids errors and mistaken payments, and can reduce fraud (Stakeholder interview, 2019).

Slow and uneven roll-out hampering adoption. Ubiquity (or near-ubiquity) was very important for the success of the NPP. It was important to have many institutions and accounts on board. However, roll out of the PayID system by financial institutions has been progressing without specific rules describing how this roll-out had to be conducted, by each financial institution. The roll-out was even slower than had originally been planned for (Stakeholder interview, 2019). Financial institutions generally launched PayID

[30] Here is a link to a video that explains how to create a PayID: https://www.youtube.com/watch?time_continue=44&v=IZjcd6CE0hY

[31] ANZ, CBA, NAB, Westpac, Australian Settlements Limited, Bendigo & Adelaide Bank, Citigroup, Cuscal, HSBC, Indue, ING Direct, Macquarie and the Reserve Bank of Australia's Banking Services Department.

on their mobile channels first, and then progressively added it to other channels. Roll-out to retail customers has been recently completed whereas the rollout to business and corporate customers is still ongoing. This different pace in deployment has hampered adoption, as institutions have avoided launching fully fledged marketing campaigns which could create confusion among customers, as not all financial service providers were ready to offer the service (Stakeholder interview, 2019).

Layered approach to the design of the NPP. Building the Basic Infrastructure and Fast Settlement Service (FSS)[32] were major projects, but internal builds of NPP participants were challenged by the complexity of the systems of the large banks (Thompson, 2019). A layered approach to the design of the NPP and its basic infrastructure made it an industry-owned utility available to all. The commercial payment services provided by separate overlays were helpful in obtaining agreement among participants of the building of the NPP (Thompson, 2019).

Importance of a good project office. The implementation of the NPP was done through the assistance of a project office working together with the 13 financial institutions that mutually own the NPP. The project office was well-resourced (Stakeholder interview, 2019). The involvement of the Project Office in the NPP implementation facilitated the participation of three wholesale service providers in the NPP project, which ensured broad reach and public legitimacy of the NPP (Thompson, 2019).

Measurements of success

High usage of the NPP reported. As of March 2019, approximately 115 million payments worth USD95 billion have been sent through the NPP (Thompson, 2019). There are currently 79 institutions connected to the NPP (13 direct and 66 indirect) and more institutions are in the process of connecting to it (Thompson, 2019).

Unique PayID registration vs unique customer registration. More than 2.8 million unique PayIDs have been registered (out of an overall population of 25 million people in Australia). This figure does not represent unique customers as some customers may have several PayIDs for their different bank accounts (Stakeholder interview, 2019).

Key themes

Accessibility of PayID

The PayID is highly accessible in Australia. Access to mobile phone numbers and email addresses is pervasive in Australia. Even in the case of a customer having multiple accounts, there does not seem to be a problem with linking different phone numbers and email addresses, as most probably customers already use several email accounts (Stakeholder interview, 2019). In the case of organisations, the OrgID allowing them to have a preferred text as a proxy, facilitates having access to multiple PayIDs.

[32] The Fast Settlement Service is operated by the RBA as a part of Reserve Bank Information and Transfer System (RITS), for settlement of NPP Payments by Full Participants and Settlement Participants.

Verifiability of PayID

Non-homogeneous verification process. PayID verification across financial institutions is a non-homogenous process. Therefore, a customer would be required to verify their telephone number or e-mail address through their institution-specific verification process. Verification of the selected identifier for an individual's PayID is done on the registration channel, either through the commercial bank's mobile app or through online banking (Commonwealth Bank of Australia, 2019). The implication of these types of modalities is that, potentially, some customers would not have verified proxy identifiers if they had registered for the account some time ago and either the identifiers are no longer current or were not available at that time. A drive to restate or renew identifiers would be essential to increase PayID market penetration beyond the current levels.

Trustworthiness of PayID

Uniqueness

Uniqueness is highly immutable. There is little concern in Australia about the uniqueness of the ID proxy being compromised (Stakeholder interview, 2019). Phone numbers or email addresses are rarely shared and usually individuals keep them for a long time. At registration of the ID proxy, each financial institution conducts a verification process to guarantee the phone number or email address corresponds to the customer's (Stakeholder interview, 2019). This process mitigates the potential risk of someone trying to link another's person phone number or email address to his/her account.

Low probability of preferred names used inappropriately. Allowing organisations to use their preferred name (OrgID) could eventually represent a risk of using the name of another institution, and, therefore, trying to mislead senders as to the real identity behind an account. However, since the registration of OrgID is made at branches where bank staff need to validate the preferred name, this scenario does not seem probable. Preferred name (OrgID) was not offered to individuals, as it would have been difficult to confirm the match up with the account holder and therefore difficult to ensure the uniqueness of the ID proxy (Stakeholder interview, 2019).

Email addresses as PayID may lead to mistaken identity. Individuals can create email accounts where they could potentially use other people's or organisations' names. This process being automatic, with no further validation from the banks, it can create misunderstanding and confuse senders as to the real identity behind the email address, leading to false positives. According to NPPA rules, if they suspect or confirm a false positive, the participating bank investigates the transaction and may place a hold on the funds (especially for new beneficiaries) to ensure that the payment is not fraudulent (risk purposes).

Privacy

Voluntary registration. Joining and/or using the PayID service is completely voluntary, therefore users join knowing which components of their information will be shared, and

individuals are willing to give out that information about themselves (NPP Australia Limited, 2018).

Facilitates privacy of account details. The use of a mobile/ landline number and email address as an ID proxy shields the underlying account details. Mobile/landline number or email address sharing are rare practices in Australia, therefore using these ID proxies do not represent privacy concerns.

Susceptible to cyberattack. A more significant privacy concern is that email addresses are vulnerable to hacking and/or other cyberattacks. Email travels across public networks and if either the email or the content is not encrypted, they can be readily accessed employing telco-to-telco backhaul communication channels, including SIM swaps and OTP interceptions. However, Australian authorities are not particularly concerned about fraud or security issues, as they are confident of the robustness of the system.

Customer experience

The customer journey is not unified across institutions. Each financial institution has their own registration process. This may affect adoption as customers having multiple accounts at different institutions may have to follow different procedures for each account, thus, creating confusion and misunderstanding. In fact, the NPPA rules for customer on-boarding don't include process flow. This was a problem identified after implementation which NPPA considers a lesson learned (Stakeholder interview, 2019).

Transferring a PayID. If a customer would like to transfer an already existing PayID to another financial institution, they can submit a transfer request from their first financial institution, and then they can proceed to register the PayID with the second/new financial institution that they wish to link their PayID to (ANZ, 2019).

Not all financial institutions offer the OrgID service. Again, this creates an uneven customer experience that may diminish trust in and adoption of the system. In general, adoption of the OrgID has been slower due to the registration process being more cumbersome than the PayID registration process (Stakeholder interview, 2019).

Gaining the trust of customers. All bank logos put/displayed together helped customers to trust adoption of the PayID service, as it was perceived as a common and ubiquitous initiative. On the other hand, some banks have not explicitly used the PayID logo in their communications and marketing materials, which has hampered the overall branding strategy, as customers may not be sure that it is the same service (Stakeholder interview, 2019). Despite Australia being a country with high access to banking and a financially literate population, NPPA members believe more education is needed for customers to fully understand and adopt PayID.

2.3. Quick response (QR) codes

Key advantages:
- QR codes are unique and robust
- Capable of storing large amounts of information

Key disadvantages:
- High latency
- Lacks strong security features, but can be developed into a strong security regime with dynamic QR codes or embedded within existing systems
- Low penetration risks exacerbating financial exclusion

What does the proxy entail?

Scannable tokenised image proxy. QR codes are two-dimensional bar codes. They consist of a pattern of any scannable colour squares that contain information, arranged in a square grid on a white background (QRcode.com, 2019). QR codes can be read with an imaging device such as a Point of interaction (POI) device, webcam or smartphone camera. A QR code may be static or dynamic. A dynamic QR code is generated with some static and some variable information, which means that it is changeable. A static code is not variable, as it is only generated with static information, and it is therefore not changeable once it has been generated. QR codes have many applications, and their use for facilitating payments is one such application.

QR code sub-use cases. Individuals can have a QR code linked to their accounts to make P2P and P2B payments, while merchants can be assigned a QR Code to accept payments. The latter seems to be the biggest use case currently in South Africa.

Easily provided to users. When QR codes are used to facilitate payments, the participating financial services provider will make it available to its customers across its platforms[33]. The individual will be provided with a QR code that will be the ID proxy for the account which may be generated in the mobile application of the FSP. This can then assist customers in making peer-to-peer (P2P) and peer-to-business (P2B) payments. An individual's QR code may be provided to them by their bank, online platform, or mobile wallet provider, which is linked to their personal account with the specific financial services provider (FSP).

1. ***Easy merchant on-boarding***. On-boarding of a merchant, payment aggregator, or other P2B institutions requires only their bank account number, which is verified by the associated bank before assigning them a QR Code. Static QR codes are more widely used by merchants to receive payments. If a customer does not have a smartphone, the merchant can scan their QR code from a decal and request the payment from the customer which the customer can confirm via USSD codes. Alternatively, the merchant POI can generate a dynamic QR code which is scanned by the consumer. The consumer's FSP's proxy link identifies the merchant/bill payment/service provider or other account number, the routing of the EFT

[33] The on-boarding process for individuals is normally through their FSP, if it participates in the use of QR codes.

transaction, and the value contained within the QR Code. The consumer then authorises the rapid EFT.

Can be affected via POI. Another option for the user-and-merchant journey entails the merchant's till point/POI/POS/smartphone scanning the consumer's QR code and routing a rapid payment authorisation request to the consumer's FSP application, for authorisation. The rapid EFT is then routed from the consumer's account. The merchant/payment aggregator provides the consumer with a unique QR code relating to the consumer's ongoing business relationship or billing.

How accessible is it?

Facilitated by internet and smartphone penetration. Most developed economies have high smartphone penetration, which facilitates the QR Code application. This is also the case in South Africa (Smartphone penetration of 80% of the population as of September 2018, according to the Independent Communication Authority of South Africa, ICASA[34] (ICASA, 2019). Unfortunately, in many developing countries, smartphone penetration is low, which limits the number of people that can access and use QR codes digitally to make payments. The same applies to low penetration of mobile phones with camera capabilities.

Internet access is another prerequisite for QR Code usage. In South Africa, 29 million people, which represents approximately 50% of the adult population, access Internet through their phones (WeAreSocial, 2019). In many developing countries, low coverage of 3G/4G networks, low internet stability, and low accessibility of QR code infrastructure can also become barriers to the expansion of QR codes. As with the email address proxy, high mobile data costs may present a further be a barrier to QR code usage.

QR codes can be saved and re-used. QR code supporting applications can send and store QR codes as a readable image for future use, without the need to be rescanned. The consumer can store the image of a personalised QR code in the requisite file format or within a beneficiary archive of the FSP. The consumer can then read the code directly from the picture file or FSP archive, which is re-validated through the proxy, to make a remote rapid EFT payment[35].

Low technological requirements. Static QR codes with printed scannable decals for merchants and readable picture files for smartphones, or even printed decals for consumers with feature phones, have relatively low technological requirements. A consumer doesn't need a smartphone to receive a payment, as long as the sender has a smartphone to make the payment. Therefore, 100% of the population can potentially receive QR payments.

Some merchants may not be equipped with the correct devices. Agents or merchants may not be equipped with QR codes or devices capable of sending dynamic QR codes. The use of

[34] Although other sources such as 2018 WeAreDigital report for South Africa suggest a 60% penetration rate in January 2019. The explanation for ICASA's statistics could be that some users may have more than one smartphone.
[35] The QR code contains the merchant subsidiary debtors account reference for direct payment of, say, electricity meters, vending machines, ride hailing and growing subscription economy options

dynamic QR code in payment services requires a POI device[36], which may represent an accessibility barrier for some merchants.

Is it verifiable?

Merchant information and PIN/ biometric verification. The merchant's name and account are embedded in the mobile application and registered centrally in the system to ensure that "if this information is modified, it invalidates the requests to purchase (RTP) created with it" (Diaz, 2018). For the static QR code P2B payment, the consumer reads the merchant's displayed QR code with their smartphone camera. Once the QR code is read, it provides the user with the name of the merchant. The user confirms that the merchant name is correct, and payment to the merchant is then validated by the user by using either biometric information, a simple password, or any other authentication method chosen by a user's FSP.

How trustworthy is it?

Uniqueness

Can store large amounts of information. Whilst conventional bar codes can store a maximum of approximately 20 digits, QR code can handle several dozen to several hundred times more information. QR codes can handle all types of data, such as numeric and alphabetic characters, symbols, or binary and control codes. Up to 7,089 characters can be encoded in one symbol which facilitates uniqueness of the QR code because the QR code can store large amounts of information that are specific to an individual file, in large number of files.

Potential for fraudulent behaviour. If a merchant uses a static QR code that is easily displayed and accessible, it may be fraudulently replaced with another static QR code, so that another party may receive the payment due to the merchant. It is difficult for an individual to recognise a QR code and link it to a person, unless the QR code is placed next to the account owner. It is therefore easy to use a wrong QR code and send the money to the wrong person. To mitigate both situations, the system usually prompts the name of the merchant or QR code linked name, so the sender can verify the transaction before validating it.

Privacy

QR codes reduce fraud. Payments made via QR codes are authenticated by unique sender identifiers to mitigate against identity theft. Additionally, QR codes ensure a more secure e-commerce user experience, as all customer need to do is read the code to make a payment without entering any sensitive bank account information.

Dynamic QR codes add an extra layer of security. A dynamic QR code also allows for additional features like scan analytics, password protection, device-based redirection, and

[36] A point of interaction (POI) device, in this case, is device that can enable users to make purchases online, in-store to make direct merchant payments or utility bill POI devices whilst using QR codes. A public POI/stand-alone POI enables consumers to do transactions even if they don't have a smartphone e.g. ATM, POS.

access management which may provide an added layer of protection to users' and merchants' personal and private information.

Customer experience

Easy to use for consumers. QR codes are easy to use, as they don't require the customer to manually enter any information to conduct a payment. This allows for more convenient payments.

Easy to use for merchants. QR code payments allow businesses to accept mobile payments without the need to invest in a point of sale terminal or any other hardware, if they use a static QR code. A static QR code may be easily displayed on a printed page for clients to make payments. Dynamic QR codes result in a less dense QR code image that is more reliable to scan for payments.

High reliability. The QR code is omni-directional, which means that it can be read from any direction up to 360 degrees. It accomplishes this task through position detection patterns located at the three corners of the symbol. QR code has error correction capability. If a QR code is partially dirty or damaged, it can still be decoded and remains usable for payments. However, data restoration cannot always be fully performed depending on the amount of dirt or damage.

High latency. On the downside, there may be a delay before a data transfer begins, following an instruction for its transfer. Therefore, both parties may need to connect to a central market player to encrypt and request decryption keys. QR code payments also rely on the smartphone camera which drains the battery of the smartphone.

Enhanced customer experience when reader embedded. The perception of customers seems to improve when the QR code reader is embedded into other pervasive platforms they regularly use, as happens in Asia with WeChat. Where customers have to download a separate app to store and read QR codes, adoption rates seem to be hampered.

Images sensitive to size manipulations. A QR code can encode the same amount of data in approximately one-tenth the space of a traditional barcode, thereby ensuring a small printout size. When a QR code is either enlarged or made smaller by an image processing tool, every module becomes distorted, and, although it may still look like a QR code, it may be difficult or impossible to read the code with the appropriate device. If the quiet zone of a QR code is invaded, it makes it difficult or almost impossible to read.

Gradual adoption to be proved. Many consumers may still lack understanding or awareness of QR codes, especially those with low literacy levels and low access to banking. Such customers may represent the next target market for South African banks who want to enlarge their customer base.

Case study 6: Mexico's Cobro Directo (CoDi)

Mexico's account penetration fairly high yet mobile payments still underdeveloped. Mexico has a population of nearly 130 million and a GDP per capita of USD8,910. Nearly 65% of the Mexican population had an account at a financial institution in 2017 (World Bank, 2018). In the same year, 32% of adults reported made or received a digital payments, according to the 2017 World Bank Global Findex (2018). This represents an increase from 29% of the population in 2014 (World Bank, 2018). According to the Mexican Internet Association, 53% of Mexicans used online banking in 2018, yet only 7% of adults used the internet to buy something online, in the past year, and only 15% of adults with a financial institution account use a mobile phone or the internet to access their account (World Bank, 2018). This shows that there is still large room for improvement in the use of payments made via a mobile phone as smartphone penetration is at 72% of the population in 2018 (We are social[37], 2018).

Banxico drive for improved financial inclusion and increased electronic payments. To a large extent, Mexico's existing payment rails have not really driven the adoption of electronic payment means in the country. The current system is dominated by high costs to businesses that have reduced the penetration of point of sale terminals; high levels of fraud and chargeback have been a serious issue for customers, financial institutions, and merchants; and the lack of control on direct debits has put off account holders from using this functionality. The introduction of an RTP layer to Mexico's existing SPEI aims to reduce these problems.

What does this proxy initiative entail?

A provider-agnostic platform to streamline RTP for small-value transactions. Cobro Directo (CoDi) is a payment platform developed by Banxico that will start operations at the end of 2019. CoDi provides users with a standardised RTP function on a 24/7 basis, i.e. an instant payment service for retail users that runs on Mexico's existing SPEI rails (Llanos-Small, 2018). This functionality is provider-agnostic and can be incorporated into mobile apps created by any company. CoDi was designed by Banxico to simplify and homogenise the experience of requesting a payment or answering a request to pay for the final user (Diaz, 2018). While the platform was not specifically designed with a specific payment use case like person-to-person or person-to-government in mind, the clearest use cases currently are person-to-business as well as e-commerce transactions. The system will only support small transactions with a monthly limit of MXN8,000 (USD420) per person.

RTPs via QR codes. The generated RTPs are sent via a mobile app or through a web browser using static or dynamic QR codes (Diaz, 2018). The application was created to also accept NFC messages, but the implementation so far is focused exclusively on QR codes.

Customer journey

Enrolment

Sign-up via bank account details. On-boarding of the merchant requires only their bank account number which is verified by the associated bank through the account holder name. This on-boarding process takes about one minute and helps mitigate the impersonation risk where a fraudster tries to use a name that is different from the one registered to the account number within the financial institution. The name and account are then embedded in the app and registered centrally in the system to ensure that when this information is modified, it invalidates the RTPs associated with it. Customers must register within their bank's CoDi app, and their information is centrally registered. Once on board, the payment sender receives the RTP through QR codes on an app or internet browser (Diaz, 2018).

Usage

There are two potential customer journeys: the payment can be initiated by the merchant or by the customer. These are discussed in turn.

Merchant-originated transactions. Once the RTP message is generated, CoDi allows for three ways of transferring it to the buyer, namely, dynamic QR codes, NFC (in the future) and through the internet. These information transfer schemes allow the system to operate face-to-face RTPs for brick-and-mortar transactions; distant e-commerce RTPs and recurrent RTP for services such as utilities or monthly subscriptions. Before sending the message, the merchant can also add fields with information, such as the amount (maximum MXN8,000), a reference number, and the validity, i.e. the period in which this payment can be processed. The amount field is not compulsory to include. If it is not included, the customer states the amount he/she is requested to pay. The customer receives the message in the bank app. Once a message is received, the apps should open onto the last step of the sending process of a traditional SPEI transfer order, in which all the information of the recipient account has been pre-populated and only the final validation by the buyer is required. The customer then checks the information and accepts the payment. The customer can also reject the payment or postpone it. The consumer validates the payment to the merchant by using a fingerprint, an iris scan, a password or any other authentication method supported by a consumer's financial service provider. This validation process is not standardised as it is each institution's responsibility to decide on its desired security level. Whichever validation method is used, it must not be disproportionately complex compared to other services provided by the institution, considering that the financial institution will have already validated the device used (Diaz, 2018).

Customer-originated transactions. The customer reads a static QR code with a smartphone and inserts the amount to be sent. The system prompts the information related to the transaction in order for the customer to verify and confirm the payment. The customer's bank validates the payment, prepares a traditional SPEI payment instruction with the appropriate flags, and the payment flows through the existing SPEI protocol. The merchant then receives a payment notification. Payments can also be revoked if both parties agree. The customer selects the payment he/she wishes to revoke, which sends a message to the merchant to agree to the reversal of the payment. If accepted, the payment is returned to its original account (Diaz, 2018).

[37] https://www.slideshare.net/wearesocial/digital-in-2018-in-mexico-86862825

Deployment process

Banxico key to success. Banxico's leadership in promoting the modernisation of payments has been key in the success of the process so far. Banxico owns the SPEI (and therefore CoDi) and developed a set of rules for all participants; it is also responsible for monitoring and enforcing compliance. Institutions participating in SPEI must enter into a contract with Banco de México that defines their rights and obligations regarding the provision of services related to this system.

Compulsory roll-out by end of 2019. CoDi will become operational in the last quarter of 2019. To meet this deadline, financial institutions are currently testing both IT and operations. Since April 2019, a pilot test with 20 selected financial institutions has been ongoing. All participants must be certified by Banxico before they can operate the service. This certification consists of a number of tests to make sure the application is working correctly. From the end of 2019, all financial institutions must offer the service, as it is compulsory. Compulsory participation was one of the keys for SPEI's success, as it ensures ubiquity of the service. On the other hand, the cost of system development is fully borne by the financial service provider (FSP), i.e. banks are obliged to develop the technology to offer the payment system to their clients (Llanos-Small, 2018). Since the pilot started, coverage in the news and a number of awareness raising campaigns are paving the way to improving customers' understanding of how QR codes work in a bid to ensure a high adoption rate of CoDi, once released.

Key themes

Accessibility of CoDi

Available to Level 2 accounts. To facilitate financial inclusion, the CoDi system will also be available to Level 2 accounts, which do not require the same level of KYC documentation.

QR code usage more likely due to high smartphone penetration. Smartphone penetration was 72% in Mexico in 2018, and 62% of the population accessed the internet via their mobile phone. Although there is room for improvement in both cases, the high familiarity with internet and smartphone use positions QR codes as an accessible means for the majority of the population. Banxico will not charge participants for the number of transactions processed through the CoDi scheme to ensure that the costs for participants are not generating incentives to constrain the use of the scheme (Diaz, 2018).

Low technological requirements. Static QR codes with printed scannable labels for merchants and readable picture files for smartphones have relatively low technological requirements. The merchant does not need a smartphone to receive a payment, as long the sender has a smartphone to make the payment.

Verifiability of CoDi

Merchant information and identity verification. The merchant's name and account are embedded in the mobile application and registered centrally in the system to ensure that when this information is modified, it invalidates the RTPs created with it (Diaz, 2018).

Multi-step verification by consumer. For the static QR code P2B payment, the consumer reads the merchant's displayed QR code with their smartphone camera. Once the QR code is read, it provides the user with the name of the merchant. The user confirms that the merchant's name is correct, and then the payment to the merchant is validated either by using biometric information, a simple password, or any other authentication method chosen by a consumer's FSP.

Trustworthiness of CoDi

Uniqueness

Can store large amounts of information. While conventional bar codes can store a maximum of approximately 20 digits, QR code can handle several hundred times more information. QR codes support all types of data, such as numeric and alphabetic characters, symbols, binary, and control codes. Up to 7,089 characters can be encoded in one symbol. This facilitates uniqueness of the QR code because the QR code can store large amounts of information that are specific to an individual file, in a large number of files.

Potential for fraudulent behaviour. If a merchant uses a static QR code that is easily displayed and accessible, it may be fraudulently replaced with another static QR code, so that another party may receive the payment due to the merchant. It is difficult for an individual to recognise a QR code and link it to a person, unless the QR code is placed next to the account owner. It is therefore relatively easy to use a wrong QR code and send the money to the wrong person. To mitigate both situations, the system prompts the name of the merchant or QR code linked name, so the sender can verify the transaction before validating it. When the payment is originated by the merchant through an RTP message, the risk of sending the money to the wrong person is reduced considerably.

Privacy

Dynamic QR codes add an extra layer of security. A dynamic QR code allows for additional features like scan analytics, password protection, device-based redirection and access management, which may provide an added layer of protection to users' and merchants' personal and private information. The sent details are encrypted and cannot be easily decrypted without the key, thus adding an extra layer of security.

QR codes can reduce fraud. Payments made via QR codes are authenticated by unique sender identifiers to mitigate against identity theft. Additionally, QR codes ensure a more secure e-commerce user experience as the customer simply scans a code to make a payment and does not enter any sensitive bank account information.

Customer experience

Affordable system. The CoDi system is free of charge for both the customer and the merchant to incentivise uptake.

Easy to use for consumers. QR codes are easy to use, as they do not require the customer to manually enter any information to conduct a payment. This allows for more convenient

payments. However, having to register for CoDi, specifically, when the customer is already registered for online banking, may introduce unnecessary friction in the customer journey, as it adds a layer of complexity.

Easy to use for merchants. QR code payments allow businesses to accept mobile payments without the need to invest in a point of sale terminal or any other hardware, if they use a static QR code. A static QR code is easily displayed on a printed page for clients to make payments. Dynamic QR codes result in a less dense QR code image that is more reliable to scan for payments.

High reliability. The QR code is omni-directional, which means that it can be read from any direction of 360 degrees. It accomplishes this task through position detection patterns located at the three corners of the symbol. A QR code also has an error-correction capability. If a QR code is partially dirty or damaged, it can still be decoded and remains usable for payments. However, data restoration cannot be always fully performed, depending on the amount of dirt or damage.

High latency. On the downside, there may be a delay before a data transfer begins, following an instruction for its transfer. Therefore, both parties may need to connect to a central market player to encrypt and request decryption keys. QR code payments also rely on the smartphone camera, which drains the battery of the smartphone.

Images sensitive to size manipulations. A QR code can encode the same amount of data in approximately one-tenth the space of a traditional barcode, thereby enabling a small printout size. When a QR code is enlarged or made smaller by an image processing tool, every module becomes distorted, and, although it may still look like a QR code, it may be difficult or near impossible to read the code with the appropriate device. If the quiet zone of a QR code is invaded, it makes it difficult or impossible to read.

Adoption remains to be seen. Many consumers may still lack understanding or awareness of QR codes, especially those with low literacy levels and low access to banking. Therefore, it remains to be seen upon introduction of the scheme if uptake will be high, and if the awareness campaigns proved successful.

2.4. Near Field Communication (NFC) technology

Key advantages:
- Low latency, i.e. very quick transaction capability
- High security built into robustness of the chip and high uniqueness. Can facilitate high security encrypted transactions

Key disadvantages:
- Multiple NFC devices needed to serve multiple accounts
- Does not easily allow for remote transactions.

What does the proxy entail?

Data transmission in close proximity. Near field communication (NFC) is a wireless technology that allows a device to collect and interpret data from another closely located device or tag that contains an NFC chip (Digital Trends, 2019). NFC employs inductive-coupling technology, in which power and data are shared through coupled inductive circuits over a very close proximity. NFC technology is like radio-frequency identification (RFID) tags, but the contactless way in which NFC devices interact also bears similarity to Bluetooth.

Seamless transactions on underlying account. NFC payment devices may come in one of the following forms: an NFC tag on a mobile phone or an NFC chip in a smartphone. NFC payment devices can transmit bank card information facilitating funds transfer to a merchant or an individual. NFC payment instruments are linked to either an individual's bank account, online platform or a mobile wallet. For example, the telecommunications company MTN provides its mobile money customers in Benin, Rwanda and Liberia with an NFC tag to facilitate person-to-business purchases on a service they call MTN MoMoPay (MTN, 2019). The NFC tag is linked to the customer's mobile money wallet, and once a payment is initiated through close contact of the NFC tag and the MTN point of interaction, the payment is validated by the customer's PIN and processed. Other popular global examples are Apple Pay, Android Pay or Samsung Pay.

Different proxy modes. NFC has three operating modes, each of which functions in a distinct way to create a proxy ID:

- ***Peer-to-peer mode***: Data commutes between two NFC enabled active devices and they can act as emitters. Any device at any time can act as the master of the conversation and control the conversation between the two devices in this mode. Users may link their participating bank account to their NFC-enabled mobile device and then use the NFC-mobile device as a proxy, when making payments to each other.
- ***Reader mode***. Data is copied from NFC tag to an NFC-enabled mobile phone, or vice-versa. The reader mode may also be used for P2P and P2B payments, where individuals use an NFC tag attached to their feature/mobile phone or an NFC-enabled mobile phone, when making payments to retailers.
- ***Card emulation mode.*** Data is copied from an NFC-enabled mobile device or NFC tag to the NFC Reader. In this mode, users may link their bank account details to their NFC-

enabled mobile device or NFC tag and then use the NFC-mobile device and/or NFC tags as a proxy, when making payments to retailers' NFC readers.

How accessible is it?

NFC can be potentially ubiquitous. NFC technology is adaptable for both feature phones and smartphones and, therefore, given the high penetration of mobile phones globally, it has the potential to include most of the population[38] (WeAreSocial, 2019).

Not dependent on data connectivity. NFC technology has the added advantage that it does not need an internet connection or data to work, in cases where sender use a passive device, such as an NFC tag attached to a feature phone. This is particularly advantageous for developing countries that do not have high internet coverage or relatively high Smartphone penetrations, as it will not result in the exclusion of individuals.

Dependent on network connectivity. Where an NFC tag is used in combination with USSD codes to validate a payment, there is a need for mobile network connectivity, which may also require the user to have airtime.

New infrastructure, proximity required. On the downside, the use of NFC technology requires merchants to have a POI to facilitate merchant acceptance of payments made via NFC technology, which may be a barrier to usage. Payment also requires the sender and receiver to be physically close to each other. Thus, NFC technology is not valid for remote payments. This reinforces the cross-cutting possibilities for a combined NFC and QR Code proxy system.

Is it verifiable?

In-person verification. It is obvious for a sender to verify he/she is sending the money to the right receiver, since the payment is done in close proximity, and the individual can verify in person whom the payment is intended for. Furthermore, the recipient can be identified via a linked proxy system, allowing for other proxies or identification factors to be triangulated, for a high level of certainty.

How trustworthy is it?

Uniqueness

Guaranteed uniqueness. Every NFC chip has a globally unique, manufacturer supplied, read-only identifier that can be read by most NFC devices. In most NFC chips, the unique ID (UID) is 7 bytes in length. An NFC tag's UID cannot be changed or erased, as it is stored in special memory in the NFC chip, which does not allow the bits to be changed. The structure of a UID is such that the first byte of the UID represents the manufacturer of the NFC chip and is

[38] In South Africa, there are 98 million mobile subscriptions, which represents 170% of the population (WeAreDigital South Africa digital report, 2019).

therefore fixed per manufacturer. The remaining bytes are variable and result in a unique UID for each NFC chip.

Privacy

Highly secure. NFC payments are dynamically encrypted – the system generates a single-use transaction key that can only be used once and expires within seconds – which makes the transaction highly secure. This is generally made through a token or random number, which replaces the bank account details. This means that the account details on the phone cannot be cloned into anything valuable to individuals engaged in fraudulent behaviour. NFC payment readers also connect to only one NFC payment device at a time and can therefore only process one payment at a time. Moreover, due to the short-range communications setup, there is less probability of unknown connections.

No extra security if in the wrong hands. On the downside, NFC-equipped devices can be used fraudulently if stolen or misplaced, when there is no additional PIN or password required to complete a transaction. This undermines security (more so than would be the case for a normal card transaction). To mitigate this risk, purchase amounts are often limited.

Additional data transmitted may undermine privacy. NFC technology also raises potential privacy concerns. It is already used to transmit merchant information, transaction detail (like items purchased) and shopper data along with payment information on each transaction. This provides valuable demographic information to both merchants and e-Wallet providers, but consumers may not be aware of the extent to which their details are shared, thereby potentially raising privacy concerns.

Customer experience

Seamless and quick. To complete a transaction, the individual only needs to place the NFC enabled phone near an NFC reader or NFC enabled device. No additional action is needed. This makes NFC the most seamless and quick ID proxy among those considered in this note.

Limited use cases. The downside is that the sender and receiver must be physically close to each other to complete an NFC transaction. Thus, NFC is not valid for remote payments (such as P2P transfers or bill payments) and is most suited for merchant payments. Even for merchant payments, the necessity for transaction limitations due to the security concerns as noted above, places limitations on the use case.

Multiple NFC linked to different accounts resulting in poorer customer experience. A further downside is that more than one device would be needed, should a person have more than one account. Moreover, if a person has more than one NFC device, only one NFC device should be placed in proximity to the NFC reader to affect a transaction. An individual would therefore either need to choose a default account to link to an NFC device, thereby avoiding the need for multiple devices, or store other NFC tags in a different place to the one used for a transaction, so as not to undermine the effectiveness of an NFC transaction. Thus, the seamlessness of the user experience may be undermined in the case of multiple accounts.

Case study 7: MTN MoMoPay

Context

The Sub-Saharan context and MTN MoMoPay. Findings from the 2017 Global Findex report, show that 66% of sub-Saharan Africa is unbanked. This means that 66% of sub-Saharan Africa does not have an individual or jointly owned account, either at a financial institution or through a mobile money provider (Demirgüç-Kunt, et al., 2018).The MTN Group has nearly 27 million active mobile money (MoMo) subscribers in 14 countries[39] (MTN Group Limited, 2019). The MTN MoMoPay service was initially launched in 2017 and has spread to 14 countries since then.

What does the proxy initiative entail?

What is MoMoPay? MoMo merchant payment services (MoMoPay) is a service that facilitates P2B and B2P payments by allowing merchants to receive payments and make refunds to customers using mobile money (MoMo). MoMoPay also allows merchants to receive online payments (MTN Group Limited, 2019). The foundational ID for MTN MoMoPay accounts is the National ID number the customer presents as KYC requirements, when opening the account. This may vary depending on the country and the existing foundational IDs. To the ID number, MTN will link the phone number or account number (they are the same) as the main ID proxy. A customer can only have one MoMo account that is linked to their mobile number, which is also their account number (Stakeholder interview, 2019).

Payment via NFC. To facilitate payments to merchants through MoMoPay, MTN initially opted for implementing an NFC system, which allowed customers to tap and pay for goods and services using an NFC tag that MTN provided them. Each tag has a serial number that has to be linked to an MTN MoMoPay account (Stakeholder interview, 2019). The customer can use the tag as a passive device from a feature phone to make payments to merchants. In order to receive payments through MoMoPay using NFC technology, merchants need a POI device (stakeholder interview, 2019).

Moving from NFC to QR and USSD code. As will be later explained later, due to cost and customer experience reasons MTN has started migrating MoMoPay from using NFC tags to using QR and USSD codes. MTN MoMoPay QR code system is based on static QR codes assigned to merchants (Stakeholder interview, 2019). Merchants display their static QR code, and MTN MoMo customers use their smartphones to scan the merchant QR code, to make a payment. MTN MoMoPay USSD code system uses a 6-digit merchant code that MTN assigns to each merchant. The customer must type the USSD code on their feature or Smart phone to make a payment. In all NFC, QR code, and USSD code systems, a merchant receives payments into their merchant payments account (MoMo account), which is linked to their selected proxy (Stakeholder interview, 2019).

ID proxy storage by MTN. ID proxies (whether NFC serial numbers, QR codes or USSD codes) are stored centrally by MTN. However, MTN must adapt to the specific regulations of the countries where it operates, resulting in ID proxy repositories hosted locally where the regulation demands so. The whole transaction and ID proxy verification operates in a

closed environment. There is no data sharing with third parties for transactions to be processed or ID proxies to be verified. In terms of payment, MTN manages this as they manage their global system for mobile (GSM) communications (Stakeholder interview, 2019).

Customer journey

NFC customer and merchant journey. A customer can go to their nearest MTN dealership to obtain an NFC tag for MoMoPay. The NFC tag is provided to customers for free. Once the customer gets an NFC tag, there is a process in which they must register their tag and link it to their MoMo wallet. Each NFC tag comes with a serial number, which the customer must register either through USSD or through the MTN app (Stakeholder interview, 2019). Once the tag is registered, the customer can stick the tag to their feature or smart phone.

Tap and pay for customers. When a customer wishes to make a payment, he/she will pay for their purchase by tapping their NFC tag onto a merchant's POI device. Then the transfer/payment must be validated by entering their MoMo PIN, which completes the transaction (MTN Benin, 2019). Once the PIN is entered, the transaction is irrevocable. For merchants to be able to accept payments via MoMoPay with customers who have NFC tags, they need to invest in a POI device from the provider (Stakeholder interview, 2019). The merchant then receives payments when customers tap their NFC tags onto their POI device, and the payments are deposited into their MoMo account immediately.

Second steps with QR Code. For customers to be able to make purchases from merchants who display a static QR code, they need to download and install the MTN application. This requires customers to own a smartphone that has a functioning camera. Once a customer has installed the MTN application, they may log in using the MoMo details to link their MoMo account to the application.

Making a QR code MoMoPay purchase. To make a purchase, customers need to scan the merchant's QR code. The app will prompt the transaction details for the customer to confirm. The customer will then enter their PIN to validate the purchase (Stakeholder interview, 2019). Once the purchase is complete, both the merchant and the customer will receive SMS confirmation. MTN has a MoMoPay API that can be used by merchants to embed requests for customers to pay (MTN, 2019). For e-commerce, merchants can initialise a dynamic QR code that is specific to the payment amount for the customer (MTN, 2019).

Using USSD codes to make a payment. When customers want to make a payment using a USSD code, the customer initiates the payment process by using their country-specific short code. The customer then enters the merchant code and confirms details of the merchant, as the merchant name is displayed. Then the customer enters the amount and validates the payment with their MoMo PIN to confirm the transaction. Once the transaction has been completed, both merchant and customer receive a confirmation SMS.

[39] Benin, Cameroon, Congo-Brazzaville, Eswatini, Ivory Coast, Guinea-Bissau, Guinea-Conakry, Ghana, Liberia, Nigeria, Rwanda, Sudan, Uganda, Zambia

Deployment process

MoMoPay deployment journey. The deployment of MoMoPay started with NFC technology and then progressed to QR codes, due to the cost implications of NFC technology. Due to MTN issuing customers with NFC tags for free, the production and distribution costs borne by MTN are very high (Stakeholder interview, 2019). NFC technology cost implications, on both the customer's and the merchant's side, include the following:

- The cost of production and distribution of the free NFC tag to the customers
- The NFC tag distribution did not involve leveraging commercial banks, which added another layer to the costs incurred for deployment.
- The POI device distribution to merchants for enabling MoMoPay acceptance.

Other ID proxies such as USSD and QR codes allowed easy payments without the high cost implications of NFC technology (stakeholder interview, 2019). They also allow expansion at a quicker pace.

Measurement of success

Currently, MTN is close to reaching 120,000 merchants with MoMoPay (Stakeholder interview, 2019).

Key themes

Accessibility of MoMoPay

Constraints from mobile money adoption. A customer needs to have a valid mobile money wallet to be able to make payments using MoMoPay. A challenge associated with the accessibility MoMoPay is that limited consumer literacy regarding available payment options may hamper customer awareness and adoption of MoMoPay. There was a 75% SIM connection penetration rate at the end of 2017 (GSMA, 2018), and unique mobile subscriber penetration in Sub-Saharan Africa stood at 45% at the end of 2018 (GSMA, 2019). In some countries, phone sharing is still a persistent phenomenon and may limit user accessibility to the MoMoPay service.

NFC tag and POI accessibility. Although NFC technology is potentially ubiquitous and not dependent on data connectivity, the accessibility of MoMoPay is also dependent on merchant acceptance of MoMoPay by means of investment in POI devices. Some challenges may be experienced in the adoption of MoMoPay through NFC, as some customers may have limited digital literacy and therefore struggle to self-register their MoMoPay NFC tag (Stakeholder interview, 2019). Furthermore, customers depend on network connectivity for payments to be made, and this may present an accessibility barrier. In 2018, 59% of mobile connections, excluding cellular IoT, were on 2G (GSMA, 2019).

QR code accessibility. In 2018, smartphone penetration in sub-Saharan Africa was recorded at 36%, and it is expected to grow progressively to 66% in 2025 (GSMA, 2019). In some countries, smartphone penetration is around 30%, which means wide adoption won't be possible in the 14 MoMoPay countries. Additionally, QR code accessibility may

be limited by internet being a prerequisite for usage. In 2018, 35% of mobile connections, excluding cellular IoT, were on 3G, and only 6% were on 4G (GSMA, 2019).

USSD codes widely used in Africa. USSD codes are almost universally accessible considering the high penetration of phones in Africa, high coverage of 2G networks, plus the fact that it does not need access to the Internet (GSMA, 2018). Moreover, 90% of all digital financial services in Africa are still performed via USSD (Denyes, 2018), which proves how easy and accessible this channel is. From the merchant side, there is no barrier to acceptance, as the merchant does not need to make any investment in hardware (Stakeholder interview, 2019).

MTN MoMoPay business case considerations. The use of QR codes for merchant payments removes the physical requirement of the NFC tag and the POI (Stakeholder interview, 2019). This change has the potential to increase the number of individuals and merchants that sign up for MoMoPay, which has been the case, as MTN has been migrating from using NFC tags to QR codes for P2B payments.

Verifiability of MoMoPay

MoMoPay verification process. The identity underlying the proxies used by MoMoPay payments is verified when the customer confirms the merchant details and enters their MoMo PIN. Once a PIN is entered, the transaction is validated and cannot be reversed (Stakeholder interview, 2019). Using the NFC tag requires in-person verification from customers, since the payment is done in proximity, and the individual can verify in person for whom the payment is intended. The same applies to QR Codes when used for in person merchant payments (Stakeholder interview, 2019). Although there is risk of someone replacing a static QR code printout for a different one, the subsequent confirmation of the transaction details and validation through the PIN mitigates it.

Trustworthiness of MoMoPay

Uniqueness

Guaranteed uniqueness with NFC tag. The serial number of NFC tag is the main and unique identifier for the customer, which is linked to their MoMo account (Stakeholder interview, 2019). It is unique due to having a unique ID (UID). MTN customers can only have one MTN account linked to their MTN phone number. Therefore, duplication of accounts is very difficult, especially if anyone attempting fraudulent behaviour already has a MoMo wallet.

QR codes can reduce fraud. QR codes can store large amounts of information and therefore maintain uniqueness for the merchant. Merchants' static QR codes may be fraudulently replaced, but this is mitigated by the customer confirming the merchant name before entering their PIN for verification.

USSD security determined by MTN security. The uniqueness and security of USSD codes are determined by how secure the MTN network is. The uniqueness with USSD codes in MoMoPay is that all the commands are stored in the SIM card's toolkit, and so the

customer does not type in the numbers explicitly but rather initiates a command from a list of menu options available in the short code specific to each country.

Privacy

Using the MoMoPay service is completely voluntary. The information from the customers and merchants is owned by MTN. Payments made via MoMoPay are authenticated by the customer by entering their PIN and this measure mitigates against identity theft. So far, MTN has not experienced any cyber-attack or security problems, so they do not consider it a major challenge (Stakeholder interview, 2019).

Customer experience

Barriers to NFC usage. MTN is convinced that NFC has the potential to offer the best customer service experience (Stakeholder interview, 2019). However, low financial literacy has been identified as the main obstacle for the adoption of NFC, since customers are not familiar with this type of technology. Customers also had to self-register, which proved a pain point in the customer journey, as customers were not familiar with this process (Stakeholder interview, 2019).

Customers do not prefer NFC. For this reason, amongst others, MTN decided to move away from NFC and focus on QR codes and USSD codes. They realised that most of their customers use USSD codes for their interactions with digital financial services, and, therefore they are trying to adapt to their needs and behaviours. They have decided, nevertheless, to continue using NFC for certain use cases such as transportation and events/ticketing services. An example of the ticketing use case for MoMoPay is given in

Box 2: Eswatini – MTN Bushfire 2019

For the MTN Bushfire 2019 in Eswatini payments were facilitated using MoMo through NFC technology. To promote going cashless, attendants of the Bushfire festival would purchase a wristband to transact with at the festival. Attendants would load money at top-up points at the festival and then tap and go to make payments at all the food and beverage stands.

To complete the transaction, attendants would tap their wristband against any trader's mobile device to make a payment. The payment would reflect on the trader's mobile device, once the transaction was completed. The service was freely available to attendants, and they did not pay any deposit/cash loading fees. If attendants still had any money remaining in their wristband after the festival, they could cash out online into their bank accounts (House on Fire, 2019).

Box 2

Challenges with QR code usage. Many consumers may still lack understanding or awareness of QR codes, especially those with low literacy levels and low access to banking (Stakeholder interview, 2019). QR codes have lower maintenance requirements for merchants than a POI device.

USSD codes easy to use for customers. Due to USSD codes being already embedded in everyday telecommunications functions, such as checking airtime balance, and purchasing

airtime or other packages from a mobile network provider, using USSD codes for payments is easily adaptable.

2.5. Biometric identification

Key advantages:
- Highest degree of robustness as a unique identifier
- Highest accessibility given near 100% coverage of biometric identifiers
- Consumers can become interoperable with different service providers

Key disadvantages:
- Cumbersome to enrol/on-board
- De-duping process may be required
- Central registry of templates vulnerable to cyber-security threats

What does the proxy entail?

Linking biographic data with identity. A biometric information ID proxy stores information based on physical attributes (fingerprint[40], eye iris, voice, facial recognition) of an individual, and links it to an identity file or proxy number to verify the individual's identity. Additionally, a biometric system may capture other biographic data or identifiers such as name, address, gender and date of birth. Biometric systems may be publicly owned or privately-owned, and enrolment may be voluntary or compulsory.

Sender identification. In contrast to other proxies, such as mobile number and email address, biometric ID proxies are used to identify the sender, not as an ID proxy to identify the receiver of the transaction. In practice, biometric ID proxies require being coupled to additional ID proxies (telephone number, bank account, email address) to identify the receiver.

Registration validated against alternative ID proxy. For individual biometric information enrolment, a user will have to go to a bank branch or enrolment centre for registration. The individual will enrol their biometric attributes, which will be linked to another ID proxy (such as a verifiable number created ad hoc or telephone number)[41]. The biometric information is submitted to a central data repository for verification of the details, submitted by comparing the biometric captured to the one stored under the ID proxy input[42].

Seamless transactions. To initiate the transaction, the individual typically uses his/her smartphone to read their fingerprint or other biometric feature and make the transaction via the phone. No other authentication is needed. In countries where online/smartphone-based transactions are limited and financial institutions rely on branch-based or agent networks, the individual would need to make use of a biometric reader at a bank branch or agent.

[40] A biometric system would capture two thumbprints and two sets of four fingers.
[41] The process of authenticating the sender generally starts by inputting the underlying ID proxy and then the biometrics of the sender are captured to verify it is the correct person.
[42] This is referred to as "1:1" matching. An alternative method for verification would be a 1:N matching where the system compares the captured biometric against the whole database. This system requires enormous processing power and takes a lot of time, reducing its viability of retail use cases in instant payments.

How accessible is it?

Base ID system facilitating universal access. The main advantage of biometrics is that it can be used as a base or reference identifier, in cases where vast segments of the population have no other identity on the proxy file[43]. This is not the case in South Africa, as all citizens have a national ID. Nevertheless, biometrics is attractive in the South African context, as every individual has potential access due to the physiological traits requirements of a biometric ID proxy system. Moreover, as discussed, an estimated 80% of the population has access to smartphones[44] (GSMA, 2017). This facilitates broad-based use of biometric readers.

No additional enrolment documentation, but cumbersome process. Enrolment onto a biometric ID proxy system may not require the ownership of an ID document, as the individual is present and serves as proof of their identification on enrolment. This is indeed identified as a key benefit of the Aadhaar identifier system in India (Sharma, 2018). On the downside, the enrolment process is generally cumbersome and costly, which may serve as a disincentive to implement it. Customer registration requires specific devices and generally takes more time than registering other ID proxies. To avoid fraud in the process of capturing biometrics, it is generally advised that the on-boarding process takes place within the premises of the financial institution, with the participation of at least two people. It is also important for all fingerprints to be registered to ensure that payments are not made on behalf of an individual through a fraudulently registered fingerprint.

Dependent on supporting infrastructure. Biometric enrolment requires unlimited electricity and internet coverage, as well as pervasive smartphone access, or biometric readers serving as POIs at bank branches and merchants. Where iris recognition is used, high-quality smartphone cameras are also required. Where supporting infrastructure is lacking, it may challenge the adoption of biometric systems. This is generally not experienced as a major barrier in South Africa.

May be undermined by high mobile data costs. High mobile data costs may exclude individuals from using a biometric system when it depends on a mobile application. As discussed, South African data costs rank 35th most expensive (out of 50) in Africa, with an average 1GB prepaid mobile data charge of USD7.84.

Is it verifiable?

Authentication against central database. Biometric ID proxies require managing a centralised database of biometric profiles against which the captured biometric can be compared.

The linking of biometric templates and biographic information enhances verifiability, especially if the biometric database is inter-operable with a country's national identity system.

[43] People without formal identity documentation could then be registered through their biometrics to build up an identity file to be able to transact on restricted products as CDD under the Risk Based Approach, or to set up a facility to transact without cards or documents on POIs, ATMs or POS.

[44] In countries where the penetration of Smartphones is low, the systems that rely on biometric readers that are integrated to an individual's smartphone may represent an access barrier.

How trustworthy is it?

Uniqueness

Guaranteed uniqueness. The use of biometric information ensures uniqueness, as no two individuals share a fingerprint and/or iris. Due to the nature of biometric information, there is a high level of immutability and therefore there are few concerns regarding changes in identifiers. The uniqueness of biometrics also significantly reduces the chance of fraud and forgery.

Some exclusion. People who, for various reasons, have unrecognisable fingerprints, may be excluded from using this form of ID proxy[45]. Thus, readers need to be widely tested before choosing a technology provider.

Privacy

Uniqueness protects but does not guarantee privacy. As a unique identifier, biometrics guarantee the privacy of the information; however, privacy may still be compromised on several fronts:

- Consumer data may be violated if the security of a database is compromised/hacked.
- Individuals may have concerns regarding who manages or owns the central database and how their personal data is protected.
- Personal biometrics are publicly exposed and could be subject to being hacked by copying a person's fingerprint or capturing a photo of their eye.
- Further privacy concerns may arise from fraud during the enrolment process, for example when the staff member substitutes an enrolee's fingerprint with that of somebody else. As discussed above, enrolment systems, however, are generally designed to limit the scope for fraud.

Customer experience

Generally positive customer experience. Since personal biometrics are always with an individual, the customer experience is generally positive. According to a VISA study revealed in January 2018[46], South African consumers find biometric technologies, such as fingerprint recognition and eye-scanning, to be much faster and easier than passwords (AYTM, 2018). 72% of those interviewed claimed to be interested in the use of biometrics to verify identity and make payments.

Moreover, unique biometric identifiers have the potential to promote the interoperability of consumers not only between different national systems, but between different FSPs, thus increasing perceived convenience and trust in the banking system.

Not all forms of biometrics widely trusted yet. Individuals may still have some reluctance to use certain types of biometric identification. In a 2018 study from the University of Texas analysing the level of comfort with biometrics usage in the USA, it was found that US citizens

[45] The population of some countries may have a genetic predisposition to have less readable fingerprints (e.g. Madagascar). Some segments of the population (mechanics, farmers, workers using their hands) also have less readable fingerprints.
[46] Conducted by AYTM Market Research

were very comfortable using fingerprints (58% of participants), whereas only 33% felt comfortable with facial recognition (University of Texas at Austin, 2018).

Case study 8: Nigeria's Bank Verification Number (BVN)

Context

The Nigerian context. According to the 2017 Global Findex report, 61% of over 190 million Nigerians are unbanked. Of those without an account at a financial institution, 18% claim a lack of necessary documentation as the primary reason for their exclusion (World Bank, 2018). This draws on the 140 million individuals in Nigeria who do not have a nationally registered identity (World Bank, 2018). The rising growth of m-commerce in Nigeria, however, highlights increasing desire among consumer to transfer value digitally, conveniently and securely (Kolawole, 2019).

What does the proxy initiative entail?

What is a Bank Verification Number (BVN)? In 2014, the BVN was launched by the CBN in collaboration with the Nigerian Bankers' Committee. The BVN is a 12-digit identification number that provides all bank and mobile money customers[47] with a unique biometric identifier, within the financial sector. It is compulsory for all customers of the financial system, and it will remain the same for life. The BVN system captures all fingerprints (442; 2 thumbs and two sets of 4 fingers), signature, and facial recognition (iris and face) (FATOKUN, 2018).

A common banking sector identifier. BVNs underpin the authentication of traditional bank ID proxies as the *foundational ID* of consumers in the banking sector. These proxies refer to bank account numbers or mobile phone numbers, both of which are required when opening an account, to both send and receive a payment. The BVN identifier allows for consumers to link a single unique identity across different accounts, at a given bank, as well as accounts between different banks or mobile money providers (Stakeholder interview, 2019). While phone numbers can be linked to one bank account or mobile money wallet, in Nigeria, BVN remains the same across all accounts and is unique (Stakeholder interview, 2019). This is an advantage over mobile phone numbers linked accounts, which permit only one number to be linked per account (Stakeholder interview, 2019).

Identity interoperability supported by centralised bank verification system. All BVNs are stored on a centralised database that is managed and aggregated by NIBSS (Stakeholder interview, 2019). Through this system, information can be pulled by banks to verify the unique identity of senders only (Stakeholder interview, 2019).

Customer journey

Enrolment

Documentation for enrolment. In addition to providing biometric information, individuals are required to provide other details such as their name and date of birth. Presenting a National Identity Number (NIN) is not compulsory. Furthermore, Nigeria has a tiered level system of accounts with varying KYC requirements applied to banks and mobile money wallets. Tier 1 (low value) mobile money account customers are exempted to have a BVN,

as a measure to increase financial inclusion (CBN, 2013). The rest of the accounts require presentation of a valid identification document which may include a valid Nigerian or international passport, Nigerian ID card, or driving licence (Stakeholder interview, 2019). Once the enrolment is complete, the customer receives an SMS with the BVN number.

Registration process and points. Existing bank customers are enrolled with a BVN through its assignment by their respective banks (stakeholder interview, 2019). Customers go through enrolment only once. But when customers have multiple accounts in different FSPs, they will have to go to each of the different institutions to synchronise the BVN with each of the accounts. Synchronisation has been particularly important given that unenrolled bank account owners would still be active and could receive deposits. Synchronisation of the BVN to the account is therefore compulsory to withdraw money from any given account.

Usage

Sender authentication. To authenticate the identity of the sender, a customer needs to provide his/her BVN. If the transaction is made at a bank branch, the sender will have to capture his/her fingerprints. The system will verify the fingerprints to see whether they match the ones stored in the customer record. No other identification is required, at the point of transaction.

Receiver identification. To send a payment, individuals are required to provide the phone number or bank account number of the receiver. The system subsequently prompts for additional information to verify and confirm the identity of the receiver i.e. name, amount, and bank (Stakeholder interview, 2019). The sender then introduces his/her PIN while the system generates a token based on the physical device number (IMEI). The combination of both confirm that the sender is indeed a real person making the payment and are who they claim to be.

Tokenisation is particularly important for payment authentication. It is employed for account-to-account transfer to shield account details from potential hackers seeking to intercept payment (Stakeholder interview, 2019). Every transaction is validated by an MNO which confirms that the owner of the device is also the account owner of the sender, and their phone number. This is checked by linking consumers to their IMEI number. Transactions through devices not identified as those registered for the account will not be processed (Stakeholder interview, 2018).

Deployment process

Progressive deployment. The deployment process of BVN was progressive, with one bank launching the service at a time. According to the stakeholder interviewed, this allowed rigorous testing before launch, and ensured the technical solution worked correctly. They did not seem to consider this progressive deployment as a barrier to adoption. The interest and buy-in of policymakers were, however, key contributors to the buy-in and successful implementation of the new system (Stakeholder interview, 2019).

[47] Mobile money customers tier accounts 2 and 3 (CBN, 2017)

Rules-based approach[48] to ensure compliance. The implementation of a rules-based approach provides the CBN with a framework that drives enrolment and processing of BVN implementation (Stakeholder interview, 2019). Within this framework, the CBN has sanctioning power.

BVN onboarding. One of the greatest challenges of deploying the BVN was the onboarding process. It was particularly challenging to bring the enrolment system to every part of the country, especially to rural areas where few or no financial service providers are present. Facilitating the enrolment process to the Nigerian diaspora has also been cumbersome.

Multiple enrolment centres facilitate de-duping. During the initial stages of the enrolment process, system breaches have taken place resulting in duplicated BVNs (stakeholder interview, 2019). This problem stemmed from enrolment processes taking place through batch processing of sending details at the end of the day to generate an ID for a customer, as opposed to online enrolment at enrolment centres . As a result, individuals were permitted to capture or enrol online at multiple centres.

Although this issue has since been resolved following the roll-out of online BVN enrolments, the initial problem of duplication highlights the importance of implementing effective and preventative de-duping procedures.

Wide distribution of enrolment centres support inclusiveness of BVN. In addition to bank branches, other enrolment centres were created to facilitate the on-boarding process, particularly in rural areas. These include bank agents and other designated enrolment centres (stakeholder interview, 2019). One particularity of Nigeria is a great diaspora who have bank accounts in the country. To facilitate enrolment of people living abroad, enrolment centres have also been opened in different countries, such as the US, UK, South Africa, etc. (stakeholder interview, 2019).

Measurements of success

Ubiquitous within the banking sector. The interoperability of the BVN among all banks in Nigeria has enabled the BVN identifier to reach a ubiquitous status, within the banking sector. As of June 2019, the implementation of the BVN Project has recorded 38 million registered BVNs (stakeholder interview, 2019).

Enhanced measurability of the banking sector. The use of BVN has enhanced the measurability of the banking sector. In other words, a clearer picture of the bank customer size can be measured, given the uniqueness of bank accounts and their holders. Prior to the introduction of the BVN, the industry was thought to hold 100 million customers. This figure has since been revised downwards to only 35 million customers, following the deployment of BVN (stakeholder interview, 2019).

Fraud mitigation. The BVN has been reported to facilitate anti-money laundering and curbing incidences of fraud (stakeholder interview, 2019). This stems from the fact that if

[48] A rules-based approach in this context refers to an approach in which participants of a given scheme or programme are obligated to maintain a particular service work-flow, service-level agreement, and communication standard (Bankserv Africa, 2019). This approach is typically advanced and enforced by the leading institution or aggregator.

fraud is committed by a customer at one bank, the common visibility of a customer's actions by all other banks via the BVN database, curbs the likelihood of money being laundered through multiple accounts at different banks. Instead, banks can more closely monitor suspicious activity for more effective STR reporting.

Multiple use cases. The BVN has enabled a number of additional benefits in the banking and non-banking world. It has been used to support upgrades of NIN system (FATOKUN, 2018). Fintechs and banks can use this to monitor credit behaviour of individuals (credit bureaus) (stakeholder interview, 2019). In addition, some government agencies have started to leverage BVN to verify staff against payroll, with a view to identifying ghost workers and eliminating them: accounts with no BVN cannot receive a salary (FATOKUN, 2018).

Key themes

Accessibility of BVN

Use of biometric information facilitates universal accessibility. The dependency of the BVN on physiological traits such as fingerprints and facial recognition implies that, in theory, it is accessible to nearly all individuals in Nigeria, from birth. Furthermore, while other proxy types may require some sort of supporting documentation to facilitate payment, the BVN is inherent to bank consumers and always on their person. This promotes greater accessibility of the identifier itself and improved consumer convenience when interacting with the financial sector.

Infrastructure and other contextual realities risk undermining rural BVN accessibility. Inadequate electricity supply at rural BVN enrolment centres reportedly undermines the efficiency and effectiveness of BVN. This has encouraged the CBN to promote the use of hand-held devices within these regions (International Telecommunications Union, 2016)[49]. Patriarchal practices in Northern Nigeria also hinder female access to BVN enrolment. This amplifies existing female exclusion to proof of address or other forms of identification that are predominantly registered in a man's name, within these regions (AFI, 2018).

Challenges for the Nigerian diaspora. The enrolment challenge for the Nigerian diaspora has been mitigated by the setup of enrolment centres in different countries, but it still represents a challenge to accessing the BVN number.

Verifiability of BVN

BVN provides the first step in identity verification. BVN is linked to all consumer bank account numbers, mobile-phone number, and biometric information (Stakeholder interview, 2019). The combination of all four identifiers ensures the validity of a consumer's identity.

Authentication against central database. Biometric ID proxies require managing a centralised database of biometric profiles against which the captured biometric can be compared. The linking of biometric templates and biographic information enhances

[49] This has highlighted a need by the CBN for biometric information to be captured via cheaper hand-held data capturing devices as opposed to brick-and-mortar structures (CBN, 2018).

verifiability, especially if the biometric database is interoperable with a country's national identity system.

BVN is immutable in nature and cannot be changed over one's lifetime. Similar to the NIN, the BVN is constant and unchangeable (Stakeholder interview, 2019). This ensures both the robustness and verifiability of the BVN for a given individual over time.

Trustworthiness of BVN

Uniqueness

Biometrics ensuring uniqueness. The use of biometric information ensures uniqueness as no two individuals share a fingerprint and iris. Due to the nature of biometric information, there is a high level of immutability and therefore there are few concerns regarding changes in identifiers.

Independent SIM registration and SIM swaps challenge immutability. BVN and SIM card registration are two separate processes. BVNs are required for bank accounts and SIM registration for MM accounts. The linking of these registrations is required in the case of mobile money to ensure the identification and authentication of consumer identity. While biometric registration for BVNs are known to be relatively robust, MNO biometric databases are not secure, and their varying quality of biometrics taken can undermine the integrity of the identity information utilised. Additional challenges observed has been the ability of a SIM registration to be compromised by the ability of SIM swaps to not only be performed outside of the control of MNOs using the SS7 backhaul telecommunications channel, but for registered SIM cards to be wrongfully reported as lost by fraudsters seeking to duplicate existing SIM cards Stakeholder interview, 2019).

BVN proxies applied to overcome SIM card vulnerabilities. Despite being of high quality, the BVN system relies on the SIM card registration with inherent vulnerabilities. To combat this issue, SIM swaps require consumers to provide documentation (court affidavit, credentials) that verify the identities of individuals as the legitimate owners of mobile phone numbers. In addition, every single transaction initiated by a mobile phone is tracked to confirm whether a SIM card has been swapped by telecommunication operators, such as mobile network operators. Furthermore, the device itself is linked to the system as well as your number. In other words, both the SIM and IMEI number act as additional BVN proxies and barriers to payment fraud (Stakeholder interview, 2019). Noticeable declines in the level of fraud and forgery losses can be associated with the security features of the Nigerian proxy identifier system (FATOKUN, 2018).

Privacy

Consumer-centric system authentication further reinforces BVN system. While the BVN system can pull the information on a client, pulls of this nature can only be done with the authorisation of account holder (Stakeholder interview, 2019). The system starts a confirmation prompt with the customer via their phone, then they can confirm sharing information. This enables customers to dictate which level of information can be seen by providers. This is a way in which the BVN system has sought to safeguard against MNO

system vulnerabilities and its reliance upon the SIM card or MNO to authenticate transactions.

Fraud linked to identifiers associated with consumer behaviour and literacy. Most fraud has resulted from lack of customer education (Stakeholder interview, 2019). More specifically, from PINs left in public places or shared with others, or fraudulent calls requesting the password/PIN which the users give out, and then money is stolen (Stakeholder interview, 2019).

Customer experience

Registration aims to be homogenous across the country. According to stakeholders, customers at every bank branch should have the same experience regarding BVN registration (stakeholder interview, 2019). The experience is considered to be positive because it leverages effort: i.e. one training programme is provided to all the banks, and if issues arise, they are easy to fix because they are common. Having NIBSS as the aggregator has been key to this solution (stakeholder interview, 2019).

Efforts to overcome contextual barriers encourage use. Basic and feature phones are still used by the vast majority of Nigerians despite the upward trajectory of Smartphones in the country (Gillwald, et al., 2018)[50]***.*** To avoid the exclusion of these individuals from BVN services, NIBSS launched a USSD service (*565#) for ease of BVN retrieval (FATOKUN, 2018). This encourages the accessibility of not only BVN among the low-income, but also the financial sector.

A different mobile phone number is required for each bank account. This implies that any change or purchase of a new you phone will require consumers to change their account details, at their respective bank before they are able to make payments once again, i.e. deactivate the previous phone for new transactions (stakeholder interview, 2019). This can represent a pain point for the consumer, especially when coupled with the need to travel to different banks to sync his/her other accounts to the BVN.

Low consumer awareness. Low public awareness and confusion surrounding the program limits the uptake of BVN. In certain instances, this confusion has led to the removal of bank account funds for lack of understanding of BVN implications (AFI, 2018).

[50] In 2017, 44.84% and 32.16% of Nigerians stated that they owned a feature and basic phone respectively (Gillwald, et al., 2018). Only 23% of Nigerians reported owning a Smartphone in the same year.

Case study 9: India's Aadhaar

What does this proxy initiative entail?

What is Aadhaar? Aadhaar is a unique biometric form of identification introduced in 2009. It consists of a 12-digit random number that is tied to an individual's biometric (10 fingerprints, two iris scans and a photograph) and demographic information (name, address, gender, date of birth).

The Aadhaar system and governance. The Aadhaar system is a centralised database, i.e. the Central Identities Data Repository (CIDR), which allows government and private-sector entities to authenticate individuals against their Aadhaar records. The Unique Identification Authority of India (UIDAI), a statutory authority under the Ministry of Electronics and Information Technology, is responsible for issuing Aadhaar numbers, and every Indian resident is entitled to one. The UIDAI collects residents' demographic and biometric information, and issues unique Aadhaar numbers, in turn (IDInsight, 2017).

Aadhaar as a proxy. An Aadhaar number becomes a financial address when an Aadhaar is "seeded" into a table called the "NPCI (National Payments Corporation of India) mapper' by anyone linking the Aadhaar to a bank account. This mapper is a directory of Aadhaar numbers and Institution Identification Numbers (IIN) used for the purpose of routing transactions to destination banks. The IIN is a unique six-digit number issued by NPCI to any participating bank. If an individual links their Aadhaar with another bank account, the NPCI mapper is overwritten with the new bank's IIN.

Payments system using Aadhaar number. Three payment systems make use of the Aadhaar number for payments:

i. ***Aadhaar Enabled Payment System (AEPS)*:** AEPS employs the UIDAI's authentication services to allow residents to conduct transactions, using only their Aadhaar number and biometrics without needing a debit card or smartphone. Business correspondents or agents employed by banks, conduct door-to-door banking through the use of micro-ATMs (handheld devices that can execute banking transactions)[51]. An Aadhaar holder's bank account must be linked to her/his Aadhaar number to gain access to Aadhaar-enabled banking services (IDInsight, 2017)[52].

ii. ***Aadhaar Payment Bridge System (APBS)*:** APBS is used for the disbursal of government benefits using Aadhaar numbers. Various government departments that provide subsidies and monetary entitlements to Indian residents make use of APBS to channel beneficiary payments. The system is hosted by the NPCI and requires only basic information for each transfer: the recipient's Aadhaar number and the bank to which the Aadhaar number is linked. Transferring money requires that eligible individuals either already have an account or open one. (IDInsight, 2017).

iii. ***Unified Payments Interface (UPI)*:** UPI is a system that facilitates banking transactions using mobile phones via the BHIM app. Launched in April 2016, UPI allows the usage of an Aadhaar number as a payment address. There are five channels through which funds can be transferred with UPI, one of which is with an Aadhaar number. UPI features are available on both smartphones and feature phones and require to be linked to a bank account. It operates with single-click, two-factor authentication and

has seen the largest growth in usage compared to the other two systems (IDInsight, 2017).

Customer journey

Enrolment

Necessary documentation for enrolment. In addition to providing biometric information, individuals are required to provide name, gender, date of birth, and residential address. These are verified against existing documents. The UIDAI has published a list of acceptable proofs of identity, date of birth, and address. There are 27 acceptable forms of proof of identity, 11 acceptable forms of proof of date of birth, and 41 acceptable forms of proof of address (IDInsight, 2017).

Alternatives available where official document proofs cannot be presented. In case an individual does not possess valid forms of proof-of-identity and proof-of-address documents, (s)he may provide a Certificate of Identity or a Certificate of Address issued by a government-approved authority. There are also alternative methods for cases where individuals cannot provide valid proof of identity and/or address documents. A procedure is specified for cases in which an individual is not able to supply biometric information (for example, because of physical disability), as the inability to supply biometric information cannot be grounds to deny enrolment. Individuals lacking functional biometrics are de-duplicated using demographic information and manual adjudication[53] (IDInsight, 2017).

Issuance of Aadhar number. If the application is successful, the CIDR issues a letter (commonly referred to as an Aadhaar card) with an individual's Aadhaar number and demographic data and delivers it to the resident[54]. Residents who have submitted their email address during enrolment may also download e-Aadhaar, which contains the same demographic information as an Aadhaar card. The e-Aadhaar is digitally signed by the UIDAI. After a public outcry in 2018 (The Economic Times, 2018), it is no longer compulsory to link Aadhaar with bank accounts

Usage

Customer provides Aadhaar number and is then verified. In order to initiate a payment, a sender provides his/her Aadhaar number as well as that of the recipient. Authentication devices are then used to collect the biometrics from the payment sender, encrypt and transmit this data, and receive authentication results, i.e. a yes or a no. Based on this outcome, the payment is then either processed or not. Authentication devices include

[51] Aadhaar holders can provide their Aadhaar number, identify their bank, and provide their fingerprint to obtain access to Aadhaar-enabled banking services such as balance enquiry, cash withdrawal and deposit, and fund transfer between Aadhaar holders without requiring other forms of authentication such as debit cards or personal identification numbers (PIN).
[52] BHIM Aadhaar Pay is the merchant version of AEPS and enables merchants to receive digital payments from customers over the counter. Merchants need to have an Android mobile with the BHIM Aadhaar app and certified biometric scanner attached with mobile phone/tablet via a USB port or micro-ATM. Both customer and merchant need to have linked their Aadhaar their bank account (IDInsight, 2017).
[53] According to the UIDAI's data, about 99.9% of the population possesses biometrics that are sufficient according to Aadhaar requirements (IDInsight, 2017).
[54] The UIDAI recommends that all other residents update their biometrics every ten years. Poor quality capture of biometrics or error in capturing demographic data at the time of enrolment may also lead the UIDAI to notify residents to update their data. Residents can update their data in three ways. Residents with a registered mobile number can update demographic data online by uploading the requisite proofs-of-identity and address. Residents can also update demographic details (except mobile number) by sending a request form by mail. Finally, an individual can update her or his biometric (or demographic) data by visiting a permanent Enrolment Centre (IDInsight, 2017).

personal computers, handheld devices, and kiosks. These are used and managed by the FSPs.

Deployment process

Principles of openness, linear scalability, strong security, and vendor neutrality. The Indian government used MapR[55] to build the project's biometric database, which can verify a person's identity within 200 milliseconds. The amount of biometric data that is collected per person is approximately 3-5MB per person, which maps to a total of 10-15 petabytes of data. Three principles are at the core of the architecture:

iv. ***Open architecture***: Building the Aadhaar system with true openness meant that they relied on open standards to ensure interoperability; the platform approach with open APIs made it possible for the ecosystem to build on top of Aadhaar APIs ,and vendor neutrality was ensured across the application components by using open and standard interfaces. The identity system was designed to work with any device, any form factor, and on any network.

v. ***Design for scale***: To achieve the massive scalability required, the programme established a network and data centre load balancing and a multi-location distributed architecture for horizontal scale.

vi. ***Data security:*** The security and privacy of one's data is a foundation of the Aadhaar system. The system uses 2048-bit PKI encryption and tamper detection using HMAC in order to ensure that no one can decrypt and misuse the data. Resident data and raw biometrics are always kept encrypted, even within UIDAI data centres. In addition, the system does not keep track of any transactional data.

Payment providers access authentication via ASAs. To gain access to the Aadhaar authentication facility, financial service providers (FSPs) must enter into a formal agreement with the UIDAI. FSPs use Authentication Service Agencies (ASAs) to establish connectivity to the CIDR and transmit authentication requests to the CIDR. ASAs transmit the CIDR's responses to authentication requests back to the FSP[56] (IDInsight, 2017).

High enrolment due to high number of enrolment officers. By 2010, UIDAI had commissioned over two hundred small and medium-sized organisations to serve as registrars across the country, and, by 2016, this number had doubled to over four hundred. Taken together, these registrars are responsible for overseeing the activities of more than 376,000 certified enrolment officers stationed at over 37,000 enrolment centres. To ensure universal sign-up rates, 60,000-80,000 small laptops which include the installed Aadhaar system are used in remote villages. Aadhaar achieved a peak enrolment rate of one million people per day in 2010, and today it still maintains an average daily rate of 700,000 individual enrolments (GSMA, 2017).

Multi-step de-duplication process. The CIDR compares the incoming enrolment data of every individual with others enrolled in the Aadhaar database to identify and vet duplicates. This de-duplication process is done in three steps (IDInsight, 2017). *Demographic de-duplication* is used to identify "trivial duplicates" or cases of duplicates arising from error or ignorance. *Biometric de-duplication* is the primary method of

[55] MapR is a data Platform that delivers dataware for AI and analytics. The MapR Data Platform allows users to store, manage, process, and analyze all data - including files, tables, and streams from operational, historical, and real-time data sources.
[56] ASAs build and maintain their connectivity to the CIDR on the basis of specifications and standards laid down by the UIDAI (IDInsight, 2017).

identifying duplicates. The UIDAI contracts with three vendors that provide automatic biometric identification systems (ABIS), which purportedly improve data accuracy. If one ABIS identifies a duplicate, it has to be verified by another ABIS, thereby increasing accuracy[57]. *Manual adjudication* takes place if step two has resulted in identifying a duplicate. In this process, the duplicates are checked to assess if a process-related issue has led to the duplication (for example, mixing of enrolment operator and resident biometrics). Finally, each case is analysed manually, and a human expert makes the final decision.

Measurements of success

Near-universal coverage. Aadhaar has rapidly become the foundational identity document of Indian residents. It has achieved near-universality in its coverage and acceptance in India. 1.2 billion residents are currently enrolled in the Aadhaar system with over 90% adult saturation in most Indian states. 271 million unique individuals used their Aadhaar to digitally authenticate themselves in February 2018. Even more use the analogue version of Aadhaar, such as a printed letter, to authenticate themselves in person. There is also evidence that Aadhaar is playing a key role in India's migration to a cashless economy (The Economic Times, 2018).

Financial inclusion via analogue Aadhaar letter high but e-KYC use still low. Aadhaar's digital usage for financial inclusion (e-KYC) has had a limited reach, while its analogue version, the letter, has been an enabler of inclusion, particularly in opening bank accounts. Almost 970 million bank accounts held by 610 million people have already been linked to Aadhaar and so have more than 800 million mobile phones subscribers. The number of successful e-KYC verifications has nearly tripled in FY2017/2018 compared with FY2016/2018, yet uptake of e-KYC in the opening of bank accounts in rural settings is still fairly low.

Government cost-savings significant. The Government of India states that USD12.5 billion has been saved in four years from FY2014/2015 to FY2017/2018 because of Aadhaar, digitisation and other initiatives. The main source of savings is deletion of fake, duplicate, or ineligible accounts. However, the government has not provided the underlying data backing the number of non-genuine beneficiaries claimed to be deleted. R.S. Sharma, who served as the Director General and Mission Director of UIDAI between 2009 and 2013, estimated in 2016 that the overall cost of Aadhaar's roll-out was USD1.5 billion (less than USD1.5 per person); in comparison, the identity authentication programme in the UK is estimated to cost USD165 per individual (GSMA, 2017).

UPI usage has grown substantially in three years. According to National Payments Corp of India data, transaction volumes reached a high of 800 million transaction which is a significant jump from the 93,000 transactions in August 2016, when it was launched. On a year-on-year basis, UPI-based payments witnessed a quadruple, or 311%, increase. Currently, 144 banks are live on UPI, compared with 21 banks at the time of its launch (IDInsight, 2018).

[57] According to UIDAI, about 99.97% of duplicates submitted to the biometric de-duplication system are correctly identified by the system.

Use of AEPS increasing yet still underutilised. According to research by InterMedia, fewer than half of all adults in India know of a micro-ATM within a kilometre of their home (2017). Data from NPCI demonstrates an almost tenfold increase in the value of transactions conducted using AEPS, which includes micro-ATM transactions, in FY2017/2018 compared with the previous year. The average size of a transaction has also grown significantly—from ₹1,400 (USD22) a month in FY2016/2017 to ₹2,527 (USD39) a month in FY2017/2018 (NPCI, 2018). In addition, the number of business correspondents or agents in rural areas has been slowly increasing, with the total number growing by 2%. About half of them use micro-ATMs to conduct transactions (Mehrotra et al., 2018). While individuals state that transactions at micro-ATMs are significantly easier than at banks, there is still a prevalence of bank usage due to recurring service downtime reported by agents.

Interoperability and neutrality ensure growth. Because Aadhaar is built on an open platform, external organisations are able to re-engineer their API to create new, connected services. These "layers" of services, known as the "India Stack", have helped to create a digital infrastructure that can provide presence-less (no need for physical authentication), paperless and cashless service delivery from anywhere in India (IDInsight, 2017)[58].

Key themes

Accessibility of Aadhaar numbers

High accessibility due to universal identity mandate. The aim of Aadhaar is to provide a permanent identity number to every resident of India, including migrants of foreign nationality, and Indian citizens living abroad. This implies that the system should be as accessible as possible to enable universality. Registrars are required to take other special measures to make sure they are able to enrol the most marginalised residents, such as senior citizens, people with disabilities, women, children, unskilled and unorganised workers, and nomadic tribes (IDInsight, 2017).

Risk of exclusion due to lack of fingerprints. Concerns have been raised regarding the dangers of Aadhaar-based biometric authentication and the risk of biometric failure. This issue is especially pertinent to the elderly and manual labourers whose fingerprints are most likely to be difficult to read. There is some concern that these inconveniences could discourage or prevent residents from accessing vital, Aadhaar-linked government services (GSMA, 2017).

Challenges for the Indian diaspora. While the enrolment process is straight forward with little paperwork required, persons applying for an Aadhaar number need to be physically present. This introduces challenges for the Indian diaspora abroad. For example, Aadhaar numbers are compulsory to file a tax return in India. Hence, in order to be able to make

[58] Through the India stack, organisations can now send payments directly to a users' bank account (Aadhaar Payments Bridge); sign documents online (eSign); allow users to transfer money via mobile (Unified Payment Interface); or share documents such as bank statements, utility bills, etc. with other service providers who need to authenticate a users' identity (Digital Locker) (IDInsight, 2018).

use of the full suite of Aadhaar use cases, non-resident Indians need to travel back home to apply (GSMA, 2017).

Verifiability of Aadhaar numbers

Authentication against central database. Biometric ID proxies require the management of a centralised database of biometric and demographic profiles against which the captured identifier can be compared. The linking of biometric templates and biographic information enhances verifiability (GSMA, 2017).

Various types of Yes/No identification possible. No personal information is attached to the verification component, and the system only responds with a yes or a no to validate the identity of Aadhaar holders instantly, anytime, and anywhere. Five distinct authentication services that are useful for payments exist: 1) authentication of demographic data; 2) usage of one-time PIN (OTP) sent to mobile phone where biometric authentication is not possible; 3) single-factor biometric authentication where either the fingerprint or iris scan of an Aadhaar holder is collected and matched with her/his biometric attributes stored in the CIDR; 4) a combination of 2 and 3 when a higher degree of authentication is needed; 5) where an Aadhaar holder is authenticated using fingerprint, iris scan and OTP authentications. This form provides the greatest degree of authentication assurance (IDInsight, 2017).
Aadhaar is immutable in nature and cannot be changed over one's lifetime. An Aadhaar number is constant and unchangeable. This ensures both the robustness and verifiability of the Aadhaar number for a given individual over time.

Continuous updates required. Updating Aadhaar data will become essential to ensuring accuracy of the information. This primarily involves updating contact details, photographs, and biometric information of children once they turn five and again at age 15, per the UIDAI requirements. Some updates are required on an ad hoc basis (updating one's address after a move) while some updates are cyclical (updating one's photo every 10 years). The proportion of people that updated their data in cases where their address had changed was low (13% according to a recent survey) (IDInsight, 2018).

Trustworthiness of Aadhaar

Uniqueness

Strong unique identifier. Aadhaar is designed to employ an individuals' biometrics, which are inherently unique. This aids in creating a database with almost no duplicates and in accurately verifying identities. Most traditional identity platforms in India are paper-based and suffer from varying degrees of duplicate identities (IDInsight, 2017).

Robustness check indicate success. One of the strongest arguments in favour of Aadhaar is the ability to create a database free of duplicate entries. The unique 12-digit number combined with an individuals' unique biometric information is meant to create a system in which each individual is only entered once. The robustness of the UIDAI system can be gauged by using three key parameters: biometric failure to enrol, false rejection rate, and false acceptance rate. According to UIDAI, in 2012, the total biometric failure rate to enrol was 0.14%, which implies that 99.86% of the population can be uniquely identified by the biometric system. For the 1.8 million residents who are an exception to this, manual

enrolment and de-duplication will take place. Aadhaar's false rejection rate stood at 0.057%. Lastly, a false acceptance rate of 0.035% implies that once the entire population is covered by Aadhaar, just under 450,000 duplicate Aadhaar numbers will have been issued (GSMA, 2017).

Privacy

Only basic information is collected. Sign-up to the Aadhaar system is voluntary. It only collects information related to an individual's name, gender, date of birth, and address. The individual also has the option of registering their mobile number and email address in the system, as these can be used to send customer notifications or to authenticate the user when accessing online services (GSMA, 2017)[59].

Consumer-centric system authentication. In the absence of data privacy laws in India, UIDAI has worked to establish its own stringent security and data privacy policies to ensure that the information collected from residents is secure. In an effort to balance "privacy and purpose", residents must give their explicit consent before any service provider can query the UIDAI database to authenticate their identity details[60]. Every individual's data is stored in UIDAI's central repository which is operated by three private-sector companies, none of which has access to the entire set of an individual's data. Features such as the Digilock ensures the protection of consumer data by granting consumers the right to grant requestors access to identifying documentation (GSMA, 2017).

Money-laundering risk due to the set-up of AEPS. The NPCI mapper, as used by AEPS, relies on periodic updates of IIN in the NPCI's table, which maps Aadhaar numbers received from banks. This mapping is volatile because multiple banks periodically update the Aadhaar numbers linked with accounts held by them. Money launderers exploit this volatility to make money transfers untraceable[61].

Concerns around payments using biometrics. Biometric data collected on an authentication device at a merchant location can potentially be stored on the device as well as the smartphone of a merchant, for a long time. Concerns over potential misuse of biometric data by private agencies has also been highlighted by the Supreme Court of India, which blocked the mandatory linking of Aadhaar numbers to financial and other services in 2017 (GSMA, 2017).

Several data leaks reported. Indians care deeply about the privacy of their data, and usage of Aadhaar for transactions has declined since 2018 due to several scandals. The mandatory usage of biometrics and other personal details to obtain an Aadhaar number has created a wave of insecurity among citizens, with growing concerns about being surveilled (Khullar, 2018). While there has been no unauthorised data disclosure of enrolment data within the UIDAI's Central Identities Data Repository, Aadhaar numbers and demographic details have been leaked on other public portals[62].

[59] UIDAI does not require individuals to register any information that could be considered discriminatory or invasive, such as religion, caste, education, income, bank details, health status, or a history of migration (GSMA, 2017)

[60] A customer who is using Aadhaar for e-KYC (e.g. registering a SIM card or opening a bank account) may also authorise UIDAI to send the service provider a digital, encrypted record of their demographic and photo information. UIDAI emphasises that this process is legally equivalent to paper-based KYC processes, but eliminates the risk of fraud and ensures that unauthorised parties are not able to tamper with or steal the data (GSMA, 2017).

[61] A money launderer can transfer money to an account linked to an alternate IIN and then re-seed the NPCI's mapper with the original IIN for the Aadhaar number, completely wiping out any trace of money to the alternate IIN (MoneyLife, 2018).

[62] A report released by the Centre for Internet and Society reported that Aadhaar numbers and demographic details of 135 million residents were disclosed on four government portals due to lack of stringent IT measures (Sinha and Kodali, 2017). The MeitY further reported that, as per the UIDAI, 210 government websites had revealed details of Aadhaar and other personal data (Lok Sabha Question, 2018). Name, address, bank account details, and Aadhaar numbers of more than a million beneficiaries of an old

Privacy initiatives try to mitigate risk. The introduction of virtual ID (VID), as discussed above, aims to tackle privacy concerns in two ways. One, it prevents agencies from linking databases using Aadhaar's unique identifier, since each agency will only have access to the temporary VID. Two, it allows an individual to have a choice about when (and with whom) they share their Aadhaar number. Limited KYC is being introduced to regulate the storing of Aadhaar numbers in different databases (GSMA, 2017)[63]. To facilitate uniqueness and security of beneficiaries in the authentication agencies' databases, the UIDAI aims to introduce a system called UID Token. With this system, each individual Aadhaar number is given a unique token ID to an authentication agency. That token is used for each transaction with that agency, but not used anywhere beyond that agency (UIDAI, 2018). This also prevents different agencies from linking databases, as each agency has a unique token for an individual that cannot be mapped to the token of that individual from another database.

Lack of security features on analogue Aadhaar letters. The overwhelmingly high use of Aadhaar in its analogue form necessitates a greater focus on adding security features to the physical copy of Aadhaar (IDInsight, 2017).

Customer experience

Individuals perceive on-boarding to be easy and universal. In a recent survey, over 80% of respondents found the enrolment process to be easy and convenient. Enrolment is free of charge. Evidence suggests that members of vulnerable communities are not less likely to enrol. This is an indication that exclusion from Aadhaar is not only low, but also not systematically biased against the poor or vulnerable. However, individuals faced greater challenges when fixing mistakes or updating information (IDInsight, 2018).

High failure rates in payments. Officially, the false reject rate – rejection of a biometric when it is actually correct – is set at a maximum of 2% for devices that get certified by the UIDAI. On the ground, however, failure rates vary widely and are found to be as high as 60%, according to a report from 2016 (The Economic Times, 2018).

Aadhaar enrolment errors higher than other form of IDs. At the peak of the enrolment process, the UIDAI was facilitating enrolment of nearly one million people a day. This raises the question whether the scale of the enrolment made the exercise vulnerable to data entry errors. Compared with the most widely used alternative, voter ID cards, the error rate in Aadhaar letters was significantly larger – in some states triple – than those on voter ID cards. The reason for the lower quality has been attributed to data entry mistakes rather than a pre-existing error in a source document. Worryingly, only 53% of those with errors actually reported trying to get the error corrected, thus undermining the data quality of the database (IDInsight, 2017).

Low consumer awareness for some features. While awareness of fingerprint authentication was over 85% in 2018, awareness of iris and OTP authentication is just

age pension scheme in Jharkhand were published on a website maintained by the Jharkhand Directorate of Social Security in July 2017 (Sethi, Bansal, and Saurav, 2017). A journalist for the Tribune reported a data breach in which she was able to buy access to a UIDAI portal. With this access, one could enter a person's Aadhaar number and obtain personal demographic data (Khaira, 2018).

[63] As per the UIDAI's notification, the authority plans to allow only authentication agencies that are required by law to receive full demographic information along with the Aadhaar number of an individual. The remaining agencies will be subject to Limited KYC and will not be allowed to store Aadhaar numbers upon authentication.

over 30% and 10%, respectively. This limits the use of the Aadhaar system for payments. Given fairly high rates of mobile penetration, the use of OTP authentication could provide relief for individuals who struggle to authenticate using their biometrics (IDInsight, 2017).

3. Concluding thoughts

The analysis outlines five potential ID proxies to consider for the development of a rapid payment system in South Africa, each with its own advantages and disadvantages. The case studies illustrate how these proxies function in practice, providing a real-life perspective on the various pros and cons associated with each proxy. It is clear that there is often a trade-off between accessibility and inclusion, security and verifiability, and factors affecting trust, such as uniqueness, privacy and user-friendliness.

Another key consideration is the cost entailed by infrastructure installation and in achieving buy-in from merchants and customers. In the end, a decision is needed that considers the balance of trade-offs in the South African context.

Despite the existence of unavoidable trade-offs, this report provides a useful first step towards navigating the landscape of ID proxies and their various applicability to the South African context. As no single proxy fits all feasibility criteria, it may be necessary to implement a combination of ID proxies simultaneously to facilitate seamless real-time payments for consumers. The effective implementation of such an initiative, however, will be conditional on a number of preconditions and recommendations to ensure optimal outcomes.

References

AFI, 2018. *KYC Innovations, Financial Inclusion and Integrity in Selected AFI Member Countries.* [Online]
Available at: https://www.afi-global.org/publications/2984/KYC-Innovations-Financial-Inclusion-and-Integrity-in-Selected-AFI-Member-Countries [Accessed July 4, 2019]

ANZ, 2019. *PayID.* [Online]
Available at: https://www.anz.com.au/ways-to-bank/more/pay-id/
[Accessed 20 June 2019].

AYTM, 2018. AYTM Market Research. [Online] Available at: https://aytm.com/ [Accessed 28 May 2019].

Bank of Spain, 2019. Pagos Inmediatos. [Website] Available Online: https://clientebancario.bde.es/pcb/es/menu-horizontal/productosservici/serviciospago/Pagos_inmediatos.html [Accessed 3 July, 2019]

BankservAfrica, 2019. *Rapid Payments Programme: Straw man,* s.l.: BankservAfrica.

Bayle de Jesse, 2017. Digital payments in the context of the evolving financial market infrastructure in the euro area. European Central Bank: Conference on Digital Payments, at the Frankfurt School of Finance & Management, 24 October 2017. Available Online: https://www.zentral-bank.eu/paym/intro/news/shared/2017-10-24_marc_bayle_speech_frankfurt-school.pdf [Accessed 3 July, 2019]

CBN, 2013. *Three-tiered Know-Your-Customer Requirements.* [Online]
Available at: https://www.cbn.gov.ng/out/2013/ccd/3%20tiered%20kyc%20requirements.pdf
[Accessed July 4, 2019]

CBN, 2017. *Review of daily mobile money wallet transactions and balance limit and bank verification numbers (BVN) requirement or mobile money wallet holders.* [Online]
Available at:
https://www.cbn.gov.ng/out/2017/bpsd/review%20of%20daily%20mm%20wallet%20transaction%20&%20bvn%20requirement%20for%20mobile%20money%20wallet%20holders.pdf

CBN, 2018. *Exposure Draft of the National Financial Inclusion Strategy Refresh.* [Online]
Available at:
https://www.cbn.gov.ng/Out/2018/CCD/Exposure%20Draft%20of%20the%20National%20Financial%20Inclusion%20Strategy%20Refresh_July%206%202018.pdf

Commonwealth Bank of Australia, 2019. *PayID.* [Online]
Available at: https://www.commbank.com.au/digital-banking/pay-id.html#terms
[Accessed 20 June 2019].

Demirguc-Kunt A., Klapper L., Singer D., Saniya A., Jake H., 2018. The Global Findex Database 2017. The World Bank [online] Available at: https://globalfindex.worldbank.org/node
[Accessed July 03, 2019]

Diaz M., 2018. CoDi: An Evolution of Mexico's Main Payment System. Central Bank Payment News, volume 1, Issue 4/December 2018. pp. 17-18. [eBook] Available at: https://cbpaymentsnews.com/assets/CBPN_Volume1/CBPN-December-2018-Vol1_4_Web.pdf

Diaz, M., 2018. Q&A: Banco de Mexico's Miguel Diaz on IP. [Online] Available at: https://www.instapay.today/insight/qa-banco-de-mexicos-miguel-diaz-ip-mexico/

Digital Trends, 2019. What is NFC? Here's everything you need to know. [Online] Available at: https://www.digitaltrends.com/mobile/what-is-nfc/ [Accessed 28 May 2019].

European Central Bank, 2019. What is TARGET Instant Payment Settlement (TIPS). Available Online: https://www.ecb.europa.eu/paym/target/tips/html/index.en.html

European Central Bank, 2019. What is TARGET2. Available Online: https://www.ecb.europa.eu/paym/target/target2/html/index.en.html

European Central Bank, 2018. TARGET Instant Payment Settlement Mobile Proxy Look-up Service Requirements. Available online: https://www.ecb.europa.eu/paym/initiatives/shared/docs/02598-tips-2018-10-15-mobile-proxy-look-up-service-requirements-v1.0.1.pdf

FATOKUN, D., 2018. *Nigeria's Progress towards the creation of a robust, trusted and inclusive Financial Services Environment.* s.l., s.n.

Finextra, 2019. EC considers regulatory push for TIPS instant payments. Available Online: https://www.finextra.com/newsarticle/33440/ec-considers-regulatory-push-for-tips-instant-payments

Gillwald, A., Odufuwa, F. & Mothobi, O., 2018. *The State of ICT in Nigeria 2018.* [Online] Available at: https://researchictafrica.net/wp/wp-content/uploads/2018/12/After-Access-Nigeria-State-of-ICT-2017.pdf [Accessed July 4, 2019]

Google Pay, 2019. [online]. Accessible at: https://pay.google.com/about/learn/ [Accessed July 3, 2019]

GSMA, 2017. Aadhaar. Inclusive by design [PDF]. Available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/gsma-aadhaar-report-270317.pdf [Accessed July 3, 2019]

GSMA, 2017. *The Mobile Connectivity Index.* [Online] Available at: https://www.gsma.com/mobilefordevelopment/resources/mobile-connectivity-index/

ICASA, 2019. The state of the ICT sector report in South Africa 2019. [Online] Available at: https://www.icasa.org.za/uploads/files/state-of-ict-sector-report-2019.pdf [Accessed 27 May 2019].

IDinsight, 2017. State of Aadhaar Report 2016-2017. [PDF] Available at: https://static1.squarespace.com/static/5b7cc54eec4eb7d25f7af2be/t/5bbd2bfe53450aea743216d2/1539124249167/State-of-Aadhaar-Report+_2016-2017.pdf [Accessed on July 3, 2019]

IDinsight, 2018. State of Aadhaar Report 2017-2018. [PDF] Available at: https://static1.squarespace.com/static/5b7cc54eec4eb7d25f7af2be/t/5bab8782104c7bbff39942b9/1537968018323/State-of-Aadhaar-Report_2017-2018.pdf [Accessed on July 3, 2019]

International Telecommunications Union, 2016. *Review of National Identity Programs.* [Online] Available at: https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/Review%20of%20National%20Identity%20Programs.pdf [Accessed July 3, 2019]

Li A., 2019. Google killing "Google Pay Send" in the UK later this year. 9to5Google. Accessible at: https://9to5google.com/2019/06/14/google-pay-killing-p2p-uk/ [Accessed July 3, 2019]

Khaira Rachna, 2018. Rs 500, 10 minutes, and you have access to billion Aadhaar details. Tribune India. [online] Accessible at: https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html [Accessed July 3, 2019]

Khullar Sodaksh, Aadhaar on Blockchain, 2018. Medium. [PDF]. Available at: https://medium.com/the-agenda-iyea/aadhaar-on-blockchain-d8f4b9db18a6 [Accessed on July 3, 2019]

Kolawole, O., 2019. Nigeria Mobile Report 2019. [Online] Available at: https://www.jumia.com.ng/mobile-report/ [Accessed July 3, 2019]

Llanos-Small K., 2019. Slow UX could hurt Mexico's CoDi payment system. Iupana. [online] Available at: http://iupana.com/2019/01/07/slow-ux-could-hurt-mexicos-codi-payments-system/?lang=en

Ministry of Justice, 2002. Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002. [Online] Available at: http://www.justice.gov.za/legislation/acts/2002-070.pdf [Accessed 28 May 2019].

Money Life, 2018. Urgent! Delink your Aadhaar from Bank Account and never share it with anyone. [online]. Available at: https://www.moneylife.in/article/urgent-delink-your-aadhaar-from-bank-account-and-never-share-it-with-anyone/55980.html [Accessed July 3, 2019]

NPP Australia Limited, 2017. *Regulations for New Payments Platform (NPP).* [Online] Available at: https://www.nppa.com.au/wp-content/uploads/2018/12/NPP-Regulations_v2.0_Public-version_2.pdf [Accessed July 3, 2019]

NPP Australia Limited, 2018. *PayID Privacy Statement.* [Online] Available at: https://www.nppa.com.au/wp-content/uploads/2018/12/PayID-privacy-statement.pdf [Accessed July 3, 2019]

Osko, 2019. *How does Osko® work for you?* [Online] Available at: https://www.osko.com.au/about-osko [Accessed 20 June 2019]

PayID, 2019. *What is a PayID?* [Online] Available at: https://payid.com.au/#what [Accessed July 3, 2019]

Pires, 2019. TIPS: Europe finally gets its own payment system. Technologist. Available Online: https://www.technologist.eu/tips-the-european-instant-payment-settlement/ [Accessed July 3, 2019]

QRcode.com, 2019. What is a QR code? [Online] Available at: https://www.qrcode.com/en/about/ [Accessed 25 May 2019].

Raul, 2019. How Much Does Mobile Data Cost Around the World? [Online] Available at: https://howmuch.net/articles/the-price-of-mobile-internet-worldwide-2019 [Accessed 28 May 2019].

Rutnik M., 2019. How to use Google Pay – A step by step guide. Android Authority. Available at: https://www.androidauthority.com/how-to-use-google-pay-890614/ [Accessed July 3, 2019]

Sethi A., Bansal S., Roy S., 2017. Details of over a million Aadhaar numbers published on Jharkhand govt website. Hindustan Times. [online] Available at: https://www.hindustantimes.com/india-news/in-massive-data-breach-over-a-million-aadhaar-numbers-published-on-jharkhand-govt-website/story-EeFlScg5Dn5neLyBzrkw1I.html [Accessed July 3, 2019]

Sharma, R., 2018. India's journey towards digital Service Delivery. s.l., s.n. Statista, 2019. South Africa: digital population as of January 2019. [Online] Available at:

https://www.statista.com/statistics/685134/south-africa-digital-population/ [Accessed 28 May 2019].

Sinha A., Kodali S., 2017. Information Security Practices of Aadhaar (or lack thereof): A documentation of public availability of Aadhaar Numbers with sensitive personal financial information. [PDF]. Available at: https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof/ [Accessed July 3, 2019]

StatsSA, 2018. Mid-year population estimates. [Online] Available at: https://www.statssa.gov.za/publications/P0302/P03022018.pdf [Accessed 28 May 2019].

The Economic Times, 2018. Cabinet gives nod to make Aadhaar voluntary for mobile, bank accounts. [online]. Available at: https://economictimes.indiatimes.com/news/politics-and-nation/cabinet-nod-to-law-amendment-for-aadhaar-seeding-with-mobile-numbers-bank-account/articleshow/67133010.cms?from=mdr [Accessed July 3, 2019].

Thompson, C., 2019. *The Development of Fast Payments in Australia.* Mexico City.

University of Texas at Austin, 2018. Consumer Attitudes about Biometric Authentication. [Online] Available at: https://identity.utexas.edu/assets/uploads/publications/Consumer-Attitudes-About-Biometrics.pdf [Accessed 28 May 2019].

UIDAI, 2019. [website] Available at: https://uidai.gov.in/

WeAreSocial, 2019. Global Digital Report 2018. [Online] Available at: https://digitalreport.wearesocial.com/ [Accessed 23 May 2019].

WeAreSocial. Digital in 2018 in Mexico, 2018. [online] Available at: https://www.slideshare.net/wearesocial/digital-in-2018-in-mexico-86862825

World Bank, 2018. *Global Findex 2017.* [Online]
Available at: https://globalfindex.worldbank.org/ [Accessed July 4, 2019]

World Bank, 2018. *Global ID4D Dataset 2018.* [Online]
Available at: http://id4d.worldbank.org/global-dataset [Accessed July 4, 2019]

World Bank, 2018. *World Development Indicators.* [Online]
Available at:
https://globalfindex.worldbank.org/https://databank.worldbank.org/data/source/world-development-indicators [Accessed July 4, 2019]

Appendix A

				Motivations for selection		
	Country	**Owner**	**System or initiative**	**Uniqueness of primary ID proxy**	**Main proponent**	**Use case**
1	Mexico	Central Bank of Mexico	Interbank Electronic Payment system (SPEI)	Mobile phone number	Central bank	P2P
	Mexico	Central Bank of Mexico	CoDi (Cobro Digital)	QR code (Tokenisation)	Central bank	P2B
2	Australia	Reserve Bank of Australia	PayID	Mobile number, email, Australian Business Number (ABN)	Central bank	P2P, P2B
3	India	Reserve Bank of India	Aadhaar number	Biometric identifier	Central bank	P2P, G2P
4	EU	European Central Bank	TARGET Instant Payment Settlement (TIPS)	Mobile number and International Bank Account Number (IBAN)	Central bank	P2P
5	Nigeria	Central Bank of Nigeria and	BVN	Biometric identifier	Central bank and Banking industry	P2P

		Bankers Association				
6	International	GPay	RT payment platform	Email address and account number	Industry	P2P, P2B, B2B
7	Africa	MTN	Mobile money	Mobile phone number	Telco	P2P, B2P and P2B
8	Africa	MTN	MoMoPay mobile money	Near field Communication (NFC)	Telco	P2B