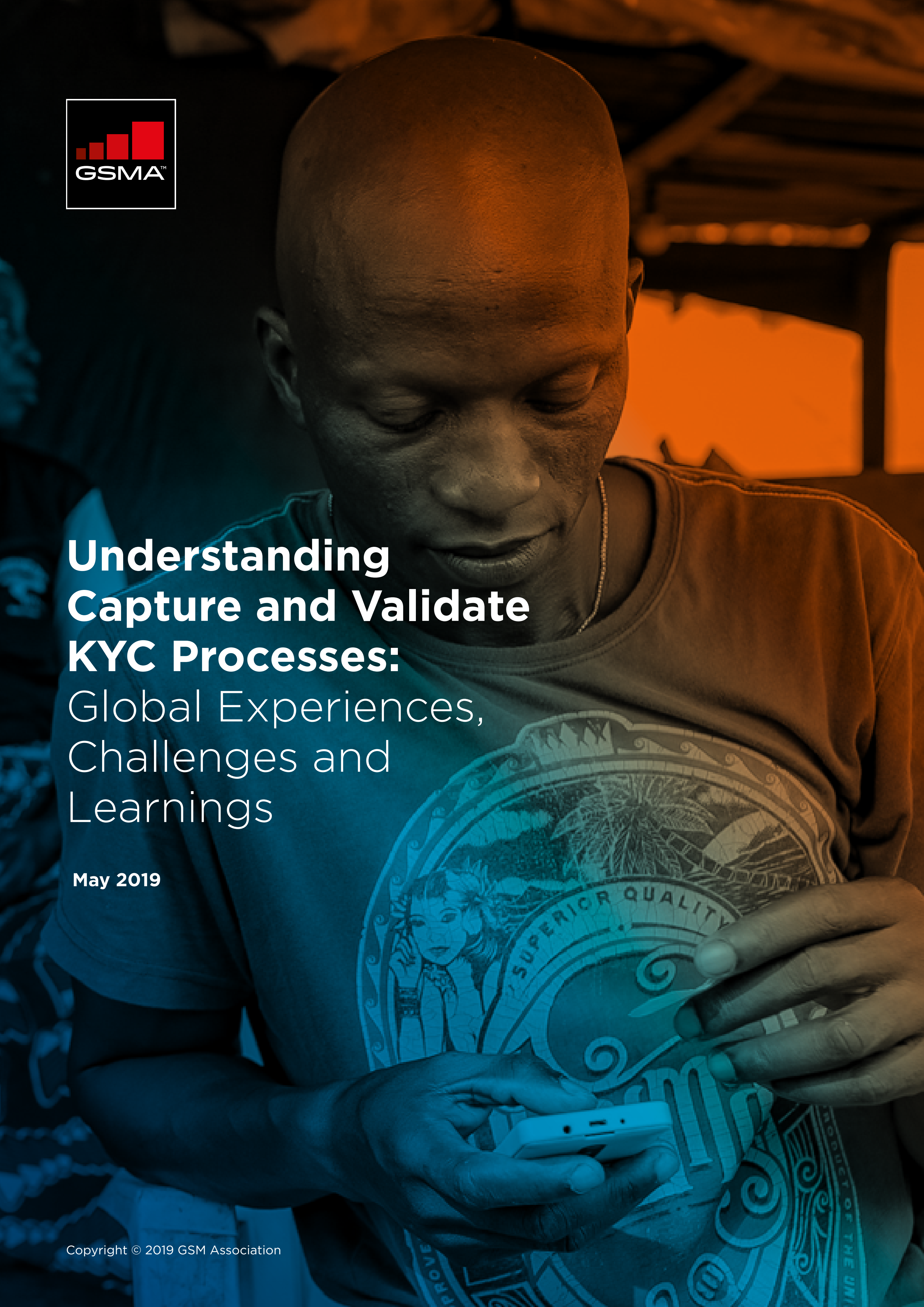


Understanding Capture and Validate KYC Processes: Global Experiences, Challenges and Learnings

May 2019

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at **www.gsma.com**

Follow the GSMA on Twitter: @GSMA

Digital Identity

The GSMA Digital Identity Programme is uniquely positioned to play a key role in advocating and raising awareness of the opportunity of mobile-enabled digital identity and life-enhancing services. Our programme works with mobile operators, governments and the development community to demonstrate the opportunities, address the barriers and highlight the value of mobile as an enabler of digital identification.

For more information, please visit the GSMA Digital Identity website at **www.gsma.com/digitalidentity**

Follow GSMA Mobile for Development on Twitter: **@GSMAm4d**

This document is an output of a project funded by UK aid from the Department for International Development (DFID), for the benefit of developing countries. The views expressed are not necessarily those of DFID.

Author:
Matt Wilson, Senior Insights Manager, GSMA
Rob Waddington, Futuresight

Contents

Executive Summary

As of December 2018, an estimated 150 governments impose Know-Your-Customer (KYC) regulations that require customers to present a valid proof of identity – often a government-issued or recognised credential, such as a national identity document or passport – before they can subscribe to mobile services. Governments take different approaches to implementing SIM registration policies, but these generally fall into one of the following three categories, as defined by the GSMA.[1]

Capture and Store

Mobile network operators (MNOs) are required to capture and keep a record of a set of personal information about the SIM user. The required information varies from jurisdiction to jurisdiction. About 85 per cent of the countries mandating SIM registration follow this approach.

Capture and Share

MNOs are required to proactively capture and share the SIM user's personal information with the government or regulator, rather than upon demand. Roughly four per cent of the countries mandating SIM registration follow this approach.

Capture and Validate

MNOs are required and enabled to validate their customers' identification credentials against a central government database, usually maintained by a government authority or regulator. Only 16 countries (11 per cent) mandating SIM registration follow this approach, of which 11 countries (seven per cent) require MNOs to use biometric-authentication processes when registering their prepaid SIM customers.

[1] GSMA (2019) 'Access to Mobile Services and Proof of Identity 2019: Assessing the impact on digital and financial inclusion'

Of these three categories, GSMA has asserted that 'Capture and Validate' processes give the highest level of assurance that the registered individual 'is who they claim to be'. This can mitigate the incidence of fraud and offers new opportunities for mobile to be used as a digital identity when accessing value added services.[2] However, these benefits must be balanced against the risk of data misuse and mobile users' rights and legitimate expectations, for example in the context of privacy and data protection. Capture and validate capabilities, therefore, do not tend to involve giving MNOs access to personally identifiable information held by government; instead, they usually allow MNOs to query a customer's identification credential against the database, and in turn the relevant authority confirms whether the credential matches the one stored in their official records.

There is also anecdotal evidence to suggest that a Capture and Validate approach – particularly when identification systems have sufficient coverage – can bring direct benefits to MNOs and other private sector organisations by decreasing administrative costs, reducing fraud, increasing revenue and widening the customer base.[3] However, to date there is little robust evidence to support these claims, nor assessments examining the impact of this approach on MNOs and the opportunities that might arise from it. This report addresses this knowledge gap and, in turn, provide shared learnings for other MNOs that might be required to implement a Capture and Validate system in the near future.

Research Methodology

Desk-based research was conducted to provide a detailed overview of the key stakeholders, institutions, regulations, legislation, systems and processes in 11 countries understood to have implemented a Capture and Validate system in Latin America, Sub-Saharan Africa and South/Southeast Asia.[4] This includes: Ecuador, Peru, Ghana, Senegal, Uganda, Bangladesh, India, Indonesia, Malaysia, Pakistan and Thailand. To help validate the available published information, stakeholder interviews were conducted to collect the views and opinions of subject matter experts and local stakeholders in each country. Short case studies on six of these countries can be found in Appendix 1.

In five of the 11 Capture and Validate countries – Pakistan, Bangladesh, Peru, Uganda and Senegal – structured interviews were conducted in-country with individuals who possess particular knowledge of, and experience with, the local Capture and Validate system. Where possible, this included telecommunications regulators, national identity authorities and MNO representatives from relevant business functions: Policy or Regulatory Affairs, Compliance, Commercial and others. A more detailed summary of the stakeholders engaged in each of these focus countries are found in Appendix 2. The insights and recommendations found in this report reflect the anonymised perspectives of these individual stakeholders, and caution has been taken not to extrapolate the findings too broadly. Furthermore, precise data related to the cost of these initiatives or their broader societal impacts (for instance, reduction in small-scale crime) was not always available and in many cases has been carefully estimated.

Case studies documenting how MNOs in each of the five countries navigated the implementation of Capture and Validate systems are found on pages 11 to 13. A summary of lessons learned from all 11 countries – related to implementation, the benefits and costs to MNOs, and current and future opportunities – are found on pages 24 to 33.

[2] GSMA (2016) 'Mandatory registration of prepaid SIM cards: Addressing challenges through best practice'
[3] See for instance: World Bank (2018) 'Private Sector Economic Impacts from Identification Systems'
[4] As identified in GSMA's 'Access to Mobile Services and Proof-of-Identity: Global policy trends, dependencies and risks' (2018, Annex 8). There were five Capture and Validate countries not included in this research project: Bahrain, China, Egypt, Hungary and Saudi Arabia.

Key insights highlighted in this report include:

Capture and Validate systems offer clear benefits to MNOs

Across all Capture and Validate countries, there was consensus amongst MNOs and other stakeholders that the Capture and Validate system had delivered a more streamlined SIM registration process, resulting in a better on-boarding experience for customers and a reduction in administration, transaction and compliance costs. Across the five countries which had also implemented biometric verification, MNOs and regulators agreed that the system had produced improvements to database management tracking and reporting. There was also anecdotal evidence to suggest a reduction in small-time criminality (as evidenced by a reduction in consumer complaints and the number of investigations into particular types of crimes).

However, the benefits of Capture and Validate systems can be costly for MNOs

MNOs in each of the five focus countries reported that they were required to cover all costs associated with implementing the new Capture and Validate system. Almost all MNOs also saw some reduction in their customer base. The amount of capital investment required – for example to purchase scanners, servers and other devices – varied according to the system approach (biometrics or biodata), the size of the retail network and the subscriber base. Operational expenditure depended largely on the MNOs training requirements, data capture and storage needs (text and/or images) and verification fees. Notably, the operational costs decreased in most countries once the new registration system was established.

The importance of careful and strategic implementation

The experiences of MNOs across all nine research countries show that when implementing a new registration system, there are several important factors that all stakeholders should consider in order to relieve some of the impacts on MNOs. Collaboration – within the industry, as well as with the government and regulators – is critical for reducing implementation costs, setting shared objectives, creating positive incentives that motivate operators, and building consensus around how to develop the registration platform. To minimise disruption and customer deactivations, governments must also ensure that mobile subscribers have access to the required identity documents (such as national identity cards), and that the national registry contains up-to-date, matching data.

Future opportunities

Capture and Validate systems provide MNOs with unique opportunities to establish digital identities for their customers and provide access to new mobile services that generate both commercial and social impact. MNOs in Pakistan are already leveraging the Capture and Validate systems to offer new identity-linked services to vulnerable segments of the population, such as social cash transfers delivered via mobile money, health services, and Internally Displaced Person cards. In other countries, MNO representatives participating in our research saw value in working with the GSMA to champion the development of new identity-linked services, or to help to address the barriers that prevent millions of individuals from accessing official proof of identity and registering for mobile services in their own name.

The Capture and Validate Landscape

Fundamentally, Capture and Validate systems are dependent on the availability of a verifiable identity scheme (a digital government registry holding the identity data of its citizens), and the ability of individuals to access the government-recognised identity documents that meet registration requirements. Where identification systems are not robust or where national identity coverage is low, there is a risk that Capture and Validate policies will exclude large sections of the population from accessing mobile services in their own name – often those who are most vulnerable or geographically remote.

The approach taken to both capture and validate a customer's identity details is dependent on the type of data that is stored in the government registry. Where the government only holds an individual's unique national identity number or other text-based details, the subscriber's details can be verified in in person, or, virtually, via a short-code or automated service. If the registry also holds an individual's biometric data, such as their picture or fingerprints, the subscriber will need to be physically present at the point of registration. Among the 11 countries explored through this research, the following systems were found to be in place.

	Capture & Validate		Non-Capture and Validate	
	Biodata	**Biometrics**	**Capture & Store**	**Capture & Share**
Verifiable ID Scheme	Indonesia Ecuador Uganda Senegal Malaysia	Peru Bangladesh Pakistan India		Thailand
Non-Verifiable ID Scheme			Ghana	

Capture and Validate: Biodata

Indonesia, Ecuador, Uganda and Senegal all operate a system which validates the subscriber's identity card data (biodata) against a central database in real-time. In Malaysia, verifications of biodata are made against a central database in batches, rather than in real-time. There are significant differences between these countries with regard to how the data is captured and the overall customer experience. Indonesia and Ecuador operate virtual identity validation – in Indonesia subscribers validate their identity details via a short code; in Ecuador subscribers use an interactive voice response system.

Indonesia

Total population:
268 million

Unique mobile subscribers:
75%

Subscription:
96% pre-paid; 3% post-paid

- 90% registered in national registry[5] (DUKCAPIL)
- NI card (KTP) includes unique identity number (NIK) + family number (KK)

Process:
Short code 4444

- All SIM cards must be validated against the central database (DUKCAPIL)
- The customer inputs a keyword, identity number (NIK) and family card number (KK) via short code to 4444 (different keywords for new vs current SIM)
- MNOs pass the data to DUKCAPIL - the NIK & KK data is validated in real-time
- MNOs send the MSISDN number to DUKCAPIL to map each MSISDN registered to an identity
- Max 3 SIMs per operator if registering via short code. If >3 SIMs required, e.g. for M2M (data), then the subscriber must register in store

Ecuador

Total population:
16 million

Unique mobile subscribers:
69%

Subscription:
77% pre-paid; 23% post-paid

- 99% coverage of identity card[6] (cedula)
- Cedula includes unique number + picture

Process:
Interactive Voice Response (IVR)

- All SIM cards must be validated against the central registry
- The customer inputs their identity or another official document and calls the operator's IVR service
- Identity is validated in real-time
- MNOs must capture full name, address, identity number
- MNOs must also link identity to IMEI handset number
- MSISDN and IMEI must be registered to a single identity to be validated

[5] Unless otherwise noted, all data on national ID penetration in this report is based on the World Bank's 2017 Global Findex survey, which asked adult participants to confirm whether they possessed a National Identity Card. See: https://globalfindex.worldbank.org

[6] ibid

Uganda, Senegal and Malaysia all require the physical presence of the customer at the MNO store. In Uganda, biometric data is also validated locally, prior to the national identity card being validated against national database.

Uganda

Total population:
38 million

Unique mobile subscribers:
44%

Subscription:
98% pre-paid; 2% post-paid

- 81% coverage of national identity card[7] (NIC)
- NIC includes unique number (NIN) + picture / fingerprints

Process:
Biometric validated locally; NID card against national database

- Customer must be present at MNO centre with national identity document
- Customers fill out a paper form and provide a signature (for financial services KYC)
- MNO scans national identity card and takes customer's photo and fingerprints and compares the two; this first validation is performed locally by the vendor
- MNO submits biodata on the card to central database (NIRA) for real-time validation
- MNO retains all details – photo, national identity document and biodata
- Max. 10 SIMs per identity (no check currently)

Senegal

Total population:
16 million

Unique mobile subscribers:
55%

Subscription:
99% pre-paid; 1% post-paid

- 72% coverage of national identity card[8] (NIC)
- NIC includes 2 numbers – new identity number and previous identity number + picture / fingerprints

Process:
NID card validated (physical presence)

- Customers must be present at MNO store with national identity document
- MNO takes a picture of the identity card, name, address and date of birth, and submit to La Direction de l'automatisation du fichier (DAF) for validation
- Once validated, DAF sends back the number of the identity card it has validated
- [SONATEL also conducts second internal check that the picture of the identity card matches the identity number provided by DAF (validated within 24 hours)]
- The MNO checks for SIMs registered to that identity
- New regulations allowed for 3 SIMs per identity (identity card and passport) for each operator (3), i.e. potential total of 18 SIMs per person.

[7] ibid
[8] ibid

Malaysia

Total population:
31 million

Unique mobile subscribers:
80%

Subscription:
66% prepaid, 34% contract

- 94% coverage of national identity card[9] (MyKad)
- MyKad includes unique numbers + advanced chip and biometrics

Process:
NID card validated (physical presence)

- Citizens have to present their MyKad in person and register at a service provider outlet.
- MNO scans MyKad with optical character recognition (OCR) / card reader and data is automatically uploaded to MNO system (no manual input) and stored (identity number, name, address, date of birth and photo)
- MNO validates the subscriber's MyKad against the national registry in batches
- If match not confirmed, MNO must contact subscriber for correct identity or deactivate
- Customers can also purchase SIMs online using their bank account as verified identity
- Maximum limit of 6 SIMs per identity

[9] ibid

Capture & Validate: Biometrics

Peru, India, Pakistan and Bangladesh all operate a validation process where, prior to issuing and/or validating a SIM card, the vendor captures a subscriber's identity card and fingerprints and submits these to a central database for real-time validation. In all cases, the central registry's function is to verify that the identification information submitted matches those on the register.

Some systems also verify the number of SIMs registered against a single identity as part of the registration process. This is generally a separate function to the registry, managed by the MNOs and the regulator. In Bangladesh, for example, the MNOs collaborated with the regulator to build the Central Biometric Verification Monitoring Platform, which holds all identity data as well as MSIDSN (the phone number associated with a single SIM card) activity. In Pakistan, MNOs link into the Pakistan Mobile Database, which was set up to enable mobile number portability and enables MNOs and subscribers to check on the number of SIMs associated with an identity.

Process

- All subscribers must present their identity card and have their fingerprints scanned
- MNOs check SIM count (Bangladesh / Pakistan)
- identity card and fingerprints are validated against a central registry in real-time
- On confirmation, subscriber's identity data is stored by MNO / Regulator
- Biometric data is only used to query a subscriber's identification and is not stored

Peru

Total population:
32 million

Unique mobile subscribers
72%

Subscription:
63% prepaid; 37% post-paid

- 98% coverage of identity card[10] (DNI)
- DNI contains biodata + unique identity number + fingerprints

India

Total population:
1.36 billion

Unique mobile subscribers
55%

Subscription:
93% pre-paid; 7% post-paid

- 90% coverage of identity programme (Aadhaar)
- Identity data includes unique 12-digit number and iris/fingerprint

Bangladesh

Total population:
165 million

Unique mobile subscribers
53%

Subscription:
98% pre-paid; 2% post-paid

- 83% coverage of identity document[11] (NID)
- Identity card contains unique number and face/fingerprint

Pakistan

Total population:
200 million

Unique mobile subscribers:
46%

Subscription:
97% pre-paid; 3% post-paid

- 79% coverage of identity document[12] (CNIC)
- CNIC contains unique number + face / fingerprint

[10] See: https://globalfindex.worldbank.org
[11] ibid
[12] ibid

Non-Capture and Validate

Consultations with local stakeholders confirmed that Thailand and Ghana do not operate Capture and Validate systems. Thailand, which has a comprehensive national identity scheme with 99 per cent coverage,[13] currently operates a 'Capture and Share' model. Customers must present their national identity document and have their picture taken in a dedicated MNO outlet, and vendors compare the subscriber's live picture with the picture on their national identity card to validate locally. MNOs then share the biodata on the card with the regulator and store the details locally. Ghana does not have a single national registry, rather there are several databases used for different functions (e.g. driving licence, health card). Customers can register for a SIM by filling out a paper form using various forms of identity in a dedicated MNO outlet or with a street vendor. Additional details on the KYC processes in each country are found in the Appendix.

[13] ibid

Establishing a 'Capture & Validate' System

Case Studies Overview

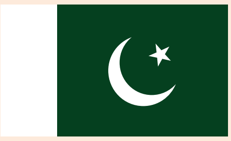
Introducing or changing mandatory SIM registration processes is logistically challenging for all parties involved, including consumers, MNOs, retail partners, the regulator, the national registry and government. The following case studies detail the experiences of MNOs in Pakistan, Bangladesh, Peru, Uganda and Senegal as they established their respective Capture and Validate systems, as described by subject matter experts. Additional insights on the costs and benefits of these systems are found in subsequent sections of this report.

All five of these countries have established a Capture & Validate system in the past three to four years, which required them to mobilise their entire subscriber base to verify their identity within a certain timeframe. When the new SIM registration process was implemented, each country differed in terms of the key factors that influence the implementation approach, namely:

- The number of mobile subscribers and active SIM cards
- The government objectives, particularly in terms of the national security situation
- The SIM registration processes already in place
- The number of MNOs, market share and competition
- Subscriber access to the required identity documents (coverage of the national identity registry)

Case Studies

Pakistan
Bangladesh
Senegal
Uganda
Peru

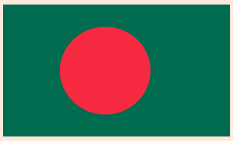


Pakistan

Context: A highly competitive market with five MNOs fighting for market share. Terrorist incidents forced nationwide biometric re-registration of 200 million SIM cards in 91 days. The national registry was at 70 per cent coverage. MNOs had only just started developing the network. The retail networks were not tested.

Outcome: 108 million SIMs registered, 27 million active SIMs disconnected

Impact on MNOs: Very High



Bangladesh

Context: A highly competitive market, with four MNOs and one dominant player (46 per cent consumer market share). Digitisation and addressing the challenges of law enforcing agencies were the key drivers. Biometric verification agreed. The national registry was at 80 per cent coverage (population 164m). Nationwide biometric re-registration implemented in 150 days.

Outcome: 117 million active SIMs re-registered out of 131 million in 150 days

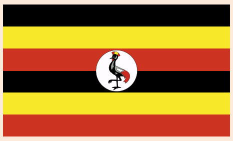
Impact on MNOs: High

Peru

Context: A steady market with 23 million unique subscribers and two dominant MNOs. An established national registry already used for verification services by other sectors (98 per cent coverage). Biometric verification for new SIMs implemented in under two years. MNOs are charged verification fees by the registry.

Outcome: Nationwide re-registration completed with minimal customer losses

Impact on MNOs: Medium



Uganda

Context: A competitive market with 15 million unique subscribers, a limit of 15 SIMs and two dominant MNOs. High profile security incidents precipitated changes to the system. Registration helped push the national registry from 30 to 70 per cent coverage. Biodata verification for new SIMs with a ban on sales for three months.

Outcome: Re-registration resulted in 10 to 15 per cent customer losses across all MNOs

Impact on MNOs: Very high

Senegal

Context: A steady mobile market with 12 million unique subscribers and one dominant MNO. No high-profile security threats. Close collaboration and consultation with government lasted over a period of three years. The dominant MNO was instructive in removing biometrics as the approach.

Outcome: Nationwide re-registration complete with approximately 6 per cent customer losses

Impact on MNOs: Low

CASE STUDY 1

Pakistan

The National Database and Registration Authority (NADRA) manages the national identity register and issues the Computerised National Identity Card (CNIC) and Smart National Identity Card (SNIC). Both cards contain a unique identity number and the owner's biometric data, including fingerprints and picture. NADRA's biometric database acts as a platform for access to a range of government services, and also operates a self-generating revenue model that charges institutions for use of their database for identity verification. It is estimated that just under 80 per cent of the adult population now has possession of a national ID card.[14]

Pakistan has seen phenomenal growth in mobile subscriptions over the last fifteen years, and the large-scale societal adoption and use of digital technologies has been a key driver of measurable economic, social and cultural value, including improved security and a greater capacity to tackle social issues.[15] In 2009, the Pakistan Telecommunications Authority (PTA) introduced the 'short code 789' process, which enabled MNOs to validate subscriber's identities against NADRA's database when activating a new SIM. Each customer was allowed to register 10 SIMs in their name, and the number of active SIMs could be verified against the Pakistan Mobile Database (PMD).

The 'short code' years (2009-2014) provided some degree of assurance that the subscriber's identity was authentic, but increasing criminal activity and terrorist attacks in 2009 and 2014 highlighted that the system was still ineffective for law enforcement. Even with the reduction in SIM allowance from 10 to five in 2012, there was still a large number of untraceable SIMs. In 2013, a government-led consultation came to the view that a validated physical presence was the only way to reduce fraudulent registration. It was agreed that all new SIMs would be registered using a Biometric Validation System (BVS), on the basis that NADRA's database – then covering about 70 per cent of the population[16] – was sufficiently robust. **The remaining 30 per cent of citizens would be required to obtain a CNIC in order to register for a SIM in their own name, potentially resulting in their exclusion from mobile services.**

[14] See: https://globalfindex.worldbank.org
[15] GSMA (2016) 'Country overview: Pakistan - A digital future'

The PTA convened all MNOs to consider how to address several critical issues, such as the limited footprint of BVS devices and NADRA's verification charges. At the time, NADRA was charging 45 rupees (approximately US $0.30) per validation; after MNOs challenged the fees they were reduced to 23 rupees for biometric and CNIC validation, and 10 rupees for biometric only. A terrorist incident in December 2014, however, forced the PTA to change the directive from using BVS for the registration of new SIMS to a nationwide re-registration exercise for all existing SIMs starting in January 2015. The timeframe for re-registration was reduced from six to three months, and the directive became part of the National Action Plan, making it legally binding.

MNOs initially collaborated to support the re-registration exercise, with each procuring 1,400 devices for shared use. However, different priorities meant that these agreements eventually broke down and the re-registration environment became both costly and highly competitive. MNOs stopped selling new SIM cards for three months so that all efforts could be put into supporting registration – by mobilising retail networks, raising awareness amongst their customer base, and sending employees to all areas of the country to help with activation. The government provided support on communications by leveraging nationwide media channels, but ultimately MNOs found that raising awareness amongst customers was one of their biggest challenges, and the time required to achieve this was underestimated. As expected, **the competitive environment favoured the largest operators who were able to leverage more resources and a larger retail network**.

The shortened timelines and high volume of customer traffic also caused significant problems with the API allowing MNOs to validate against NADRA's database, resulting in frequent downtime and an impact on MNOs ability to re-register customers. MNOs suggested that in these situations, it would be beneficial for national identity authorities to have service agreements in place that limit technical disruptions and system disruptions. The timelines for procuring and testing the BVS devices was also very short, which led to multiple re-verification models and increased costs for MNOs. The initial roll out of the system in cities obscured the problems found in the rural areas – in particular, electricity power outages meant the BVS devices were not always operational.

Engaging and training the retailer network on the new Capture and Validate process was also a huge undertaking for MNOs, and the time needed for completing this was severely underestimated. The shortened timeframes led to inflated incentives for retailers and MNO staff conscripted to various locations around the country. **MNOs suggest that a minimum of nine months should have been allocated for the re-registration exercise: three months for the cities, another three months for suburban environments and three months for rural/remote areas.**

Despite the cost to MNOs, the Government provided virtually no financial incentives and operators continued paying SIM tax throughout the registration period. Stakeholders interviewed through our research suggested that government could have reduced the financial burden on MNOs through the removal of SIM tax during the re-registration exercise or by contributing resources from the Universal Service Fund, which MNOs contribute 1.5 per cent gross revenue every year.

By the end of the re-registration period, the five mobile operators had biometrically verified an estimated 108 million SIMs,[17] and according to the PTA this number grew to 115 million SIMs by the following year (against 45 million unique CNICs). In total, an estimated 27 million active SIMs were disconnected.[18]

[16] According to subject matter experts interviewed through this research project
[17] GSMA (2016) 'Mandatory registration of prepaid SIM cards: Addressing challenges through best practice'.
[18] ibid

CASE STUDY 2

Bangladesh

In 2008, the National Identity Document (NID) was issued by the Bangladesh Election Commission (BEC) to all Bangladeshi citizens aged 18 and above and resident of an electoral area. The card contains the citizen's unique number and biometric details, including fingerprints and a photo. The BEC manages the NID database (NIDD) and provides KYC validation to 115 entities for different public and private sector services. Coverage of the NID is estimated to be at 83 per cent as of 2017.[19]

Until 2014, recording and validating the details of new mobile subscribers in Bangladesh was complicated by the low coverage of official identity documentation. In that year, the government tried to push for verification of all SIM card holders against the NID and discovered that over 60 per cent of customers had registered for a SIM with a fake identity document. Consultations took place between law enforcement, the Bangladesh Telecommunication Regulatory Commission (BTRC) and MNOs to find an effective solution, and biometric validation – requiring the physical presence of the subscriber – was concluded as the only viable approach.

The project was designed and implemented by a dedicated team, led by the then State Minister of Post and Telecommunication Division and executed by the BTRC, the Association of Mobile Telecom Operators of Bangladesh (AMTOB) and MNOs. There was also strong support from government, particularly the National Telecommunication Monitoring Centre (NTMC), who felt incentivised to reduce the amount of crime carried out over mobile networks. **This close collaboration helped address a myriad of technical, procedural, legal, societal, financial and commercial issues and helped motivate engagement from MNOs.** During initial consultations, the BTRC conducted a survey to assess the project's potential for success, and to predict impact on customer losses. The result of the survey – which predicted a potential 20 per cent reduction in active SIMs – was considered acceptable by stakeholders given that the process would ensure that all mobile subscribers had an up-to-date identity registered against each SIM.

It was agreed that MNOs would supply Biometric Verification Devices to each of the 120,000 retail outlets throughout the country, and initially MNOs agreed that they would collaborate by sharing the cost of the devices and running a single technical platform. However, this consensus broken down and each operator had to build and pay for their own system and scanning devices individually. The result was increased costs and shortened timeframes for device procurement and testing. The Central Biometric Verification Monitoring Programme (CBVMP) was conceived shortly after this to oversee the data flow, provide validation and control the number of SIMs per person (maximum of 15) across all operators. The platform was managed by BTRC, but built and paid for by the MNOs. Validation fees, notably, were set low at just one cent per request.

[19] See: https://globalfindex.worldbank.org

As in Pakistan, a key concern amongst MNOs was the potential for re-registration to favour the dominant operator(s) with the technical infrastructure and manpower to reach their customers quickly and more effectively than the smaller MNOs. As each SIM needed to be registered, it was considered likely that the 'main' numbers would be registered first and other SIMs would be forgotten. To help alleviate these concerns, it was eventually agreed that the scanning devices would be shared without discrimination. Initial tests of the new SIM registrations exposed a host of issues with the validation process, with just 26 per cent of registration attempts successfully validated in the first month. However, after another four weeks of testing the success rate had risen to 90 per cent. Re-registration was planned to start on 1 February 2016 and complete by 30 April.

Motivating the population to re-register was one of the biggest challenges faced by operators. This required MNOs to deliver extensive marketing and communications activities for their customers, including putting on events, offering incentives and even visiting customers door-to-door. There was, as one operator said, 'a complete shutdown of our operations to focus on this – we were so concerned at losing customers that we threw every resource on [re-registration activities]'. The government provided extensive support to raise awareness of the re-registration exercise, with ministers making televised appeals. However, the amount of time, effort and cost required to motivate the population to register was underestimated by all parties – MNOs, the BTRC and government. As the deadline grew closer, the registration outlets became packed and the NID database API was unable to cope with the demand. Seeing that many customers were left queuing in the heat for hours to ensure their SIMs were not disconnected, the government extended the registration deadline by another month.

The CBVMP requires retailers to fill out a SIM application form (SAF) which records the customer's name, address, date of birth, NID number and expiry date. These details are checked against BTRC and the NID databases, and if both validations are correct a SIM card is issued. Verification must be in real-time and no biometric data can be stored for data protection purposes.

The SAF was originally paper-based, which lead to a number of problems. Retailers were incentivised to complete forms quickly, as commissions were based on the number of SIMs registered rather than the accuracy of their form filling. The BTRC estimated 30 per cent of forms were inaccurate or incomplete, potentially leading to fines of $50 per form. The forms also needed to be scanned so that both soft and hard copies could be stored for ten years, leading to warehouses and servers full of these details at considerable cost. **In 2017, MNOs successfully petitioned BTRC to allow electronic SAFs – these reduced costs, removed the threat of fines, and ensured the process is frictionless and transparent (each retailer is tracked and accountable for each e-SAF).**

As there was not full nationwide coverage of a biometric NID, MNOs could register customers using alternative identity documents, although the SIM would be deactivated if they did not produce the NID within six months. Corporate customers, contract subscribers and foreigners were also catered for. **This level of planning and flexibility minimised the amount of SIM deactivations – just 14 million out of a total of 131 million.** According to the BTRC, 84 million SIM cards (out of a total of about 131 million) were re-registered by the end of April 2016. By the May deadline, another 12.5 million subscribers who were unable to complete the registration process due to long queues or technical challenges were also registered. In total, 117 million SIMs had been re-registered according to BTRC; by all accounts, this was an astonishing achievement given the short time frame.

Stakeholders suggest that MNOs still face some challenges with the Capture and Validate process, such as mismatches with the NID database or system downtime. MNOs noted two to three days of downtime per month, which affect an estimated 100,000 new SIM activations each month, and may ultimately lead to a reduction in tax revenue for the government ($1.176 per SIM). MNOs would like to see higher levels of investment into the NID database to address some of these issues and currently contribute US $6,000 per month for the maintenance of CBVMP.

CASE STUDY 3

Peru

The National Registry of Identification and Civil Status (RENIEC) is an autonomous entity with a mandate to ensure that all Peruvians over the age of 17 are on the national register and carry a national identity card (DNI). The card contains the individual's name, surname, date of birth, marital status, voting number, a unique identification code number (CUI) and their biometric information (fingerprint). By 2017, coverage of the DNI was estimated to be at 98 per cent.[20]

The DNI is the primary identity document in Peru and is used for voting, government interactions (e.g. tax and social security) and commercial identification (e.g. opening a bank account or registering a mobile SIM card). All DNI data is centralised and stored at RENIEC, which charges a fee for each verification request against their database. In 2013, RENIEC started manufacturing electronic DNIs (DNI-e), containing a cryptographic chip that allows for digital signatures and faster processing of information. However, the platform enabling electronic delivery of government services is not yet in place, and the DNI-e is both more expensive and has a shorter lifespan than the current DNI. Take up of the DNI-e card has been very slow and RENIEC has, reportedly, stopped promoting the DNI-e card.

SIM registration became mandatory in Peru in 2007, with MNOs asked to captured and store a copy of subscribers' DNI when purchasing a new SIM. Two years later, the Supervisory Agency for Private Investment in Telecommunications (OSIPTEL) directed that all mobile subscribers must re-register their SIMs by visiting a retail store and leaving a paper copy of their identity document. The main driver for this decision was number portability – until this time, customers were unable to retain their mobile number when switching from one operator to another as there was no way to verify their identity – but the government also saw this as an opportunity to enhance national security. OSIPTEL required operators to keep hard and digital copies of identity documents, and OSIPTEL would conduct spot inspections and issue fines if the record could not be found.

In 2014, in an effort to further improve security, the government directed that all customer identities had to be validated against the RENIEC database, rather than only being stored. MNOs investigated different approaches for this, with one MNO hiring a third party to validate against RENIEC's database. However, RENIEC disallowed this approach,

[20] See: https://globalfindex.worldbank.org

and mismatches between MNOs' and RENIEC's databases resulted in lines being suspended, often for small typographical errors.

In 2015, OSIPTEL began receiving complaints from the public about extortion calls, often from prison inmates. This became a widely publicised issue, leading the government to respond by introducing a mandate for biometric validation. OSIPTEL directed that all mobile users must register their SIM cards with operators by presenting their DNI and having their fingerprints scanned so that these details could be validated in real-time against RENIEC's database. During the validation process, RENIEC would reply to MNOs with the subscriber's biodata, including first name, last name, identity number, DNI expiry date and any restrictions (under age, criminal record, etc). Mobile subscribers were allowed to register as many SIMs against their DNI as they liked, but needed special written permission when registering more than 10.

The MNOs were given two years to implement this directive. While OSIPTEL was involved in managing the relationship between RENIEC and operators during the 2014 validation phase, once the directive to implement biometrics was given these consultations ended and MNOs were left to navigate re-registration activities on their own. This involved building the infrastructure to enable real-time validation, as well as delivering nationwide campaigns to ensure all mobile subscribers were aware of the need to re-register. Operators were responsible for all associated costs, and received little support and no financial incentives from the government.

RENIEC initially controlled the procurement for the API integration and biometric scanners. This resulted in significant technical integration problems, and MNO stakeholders suggested that they would have preferred an open tender market. **Insufficient time was also given to testing the technology prior to going live,** and representatives from one MNO estimate that this affected 80 per cent of new SIM sales in the first month of re-registration, and 15 per cent of sales overall during the re-registration period due to technical problems.

Contrary to Pakistan and Bangladesh, there was less consensus among stakeholders in Peru concerning the value of implementing a biometric verification system (BVS). **Some noted that the BVS has raised the cost of SIM registration and required operators to make considerable investments in technical infrastructure; these additional costs are, ultimately, passed on to the customer.** For instance, MNOs are charged a fee every time they attempt to validate customer details against RENIEC's database, and this cost increases if biometric mismatches or technical challenges require them to attempt this validation multiple times. Representatives from two MNOs estimated that their organisations each paid about $3 million for validation fees in 2017. The following year, this fee was incorporated into Congress' budget as it was argued that the SIM registration exercise was a security issue and of national interest, and therefore should be finance by government. However, after a successful appeal by RENIEC the fees were re-established, and MNOs have budgeted another $3-4 million to cover fees in 2019.

Stakeholders also suggested that the use of biometrics has the potential to exclude some segments of the population whose fingerprints may be worn or harder to scan and validate, such as the elderly and those with manual jobs. Alternative mechanisms suggested as being more inclusive, such as facial recognition or simply face-to-face questions, are currently not allowed by law. Some MNO representatives suggested that the BVS process can also impact sales volumes due to the fact that it requires customers to be physically present at a retail location. Overall, stakeholders interviewed were interested in exploring other digital solutions for customer validation, such as those currently used by banks for their KYC processes.

CASE STUDY 4

Uganda

In 2015, the National Identification and Registration Authority (NIRA) launched a national registration programme to establish a national identity register and issue all Ugandans with a national identity card (NIC). The card contains a unique identity number (NIN) and biometric data (fingerprints and picture). By 2016, coverage was at about 30 per cent, but this rose sharply to 70 per cent in 2017 due to a directive by the Uganda Communications Commission (UCC) that all SIM cards would be deactivated unless registered with the NIC.[21] As of 2017, the World Bank estimates that 81% of Ugandans own a national identity card.[22]

Mandatory SIM registration in Uganda began in 2015 with a requirement for all new mobile subscribers to provide their NIC or NIN to MNOs, who then verified these in batches against NIRA's database. Because the national identity scheme's coverage was limited at the time, the system was difficult to implement and customers without an NIC were forced to acquire SIMs through other people. It was also difficult to enforce a law that limited the number of SIMs registered per identity to 10, as there was no means of counting active SIMs across all of the operators. In 2017, a high-profile murder led the UCC to issue a directive that all MNOs must register all active SIM cards against a valid identity within nine months, or risk having the SIM deactivated. MNOs introduced a short code for customers to provide their NIC, which MNOs would validate through NIRA. At the time, the national registry was not ready for large scale validation. Although the directive helped incentivise citizens to register for a CNIC (causing coverage to rise sharply to 70 per cent) NIRA's database contained a lot of information that was out of date or inconsistent. In addition, NIRA's technical capacity could not meet the NIC verification demands from MNOs, who were under intense pressure to quickly re-register millions of their customers or risk losing them to competitors. There was a 'total shutdown' of regular business for all MNOs during this period. By the end of 2017, the UCC claimed 98 per cent re-registration across a subscriber base of 23.5 million.

After other high-profile murders at the end of 2017 and in 2018, the Government and MNOs agreed that a new Capture and Validate system was necessary,

[21] World Bank (2017) 'The State of Identification Systems in Africa'
[22] See: https://globalfindex.worldbank.org

requiring the NIC cardholder to be validated in-person using biometrics. The new system was rushed into service in March 2018 when UCC banned all new SIM sales, compelling MNOs to launch another full-scale re-registration process without the necessary time for planning and testing. MNOs were given 90 days to get their systems up and running but, in effect, strict timelines were self-imposed to limit the ban's impact on business. One MNO reported that the ban affected up to 10,000 new SIM registrations per day, and despite largescale nationwide campaigns operators lost between 10 to 15 per cent of their customer base during this phase. This had a significant impact on revenues, which **MNOs think this could have been mitigated if they had longer timeframes to plan effective registration campaigns, and phased these across different territories.**

UCC and NIRA procured the initial batch of biometric devices and sold them to the MNOs, and the quick turnkey API solution developed by NIRA led to considerable issues with connectivity and downtime. Sufficient lead times for MNOs to develop and test their own infrastructure in conjunction with NIRA would have led to better performance and a reduction in hardware costs.

UCC also issued two other important directives: first, that all SIMs must be registered in brick and mortar outlets (street vendors were no longer permitted); and second, that all airtime had to be procured and sold electronically (airtime via scratch cards was banned). Therefore, all new SIMs are now registered at service centres where an agent scans the NID card, takes a photo of the subscriber, and verifies the two locally. The card data is then sent to NIRA for real-time validation, and the MNO retains all registration details (biodata on card, fingerprints and photo). The directive that MNOs can only register SIMs through bricks and mortar outlets has led to significant changes in the way MNOs organised their sales networks. Consultation and collaboration with UCC on such directives at the outset would allow more time for strategic planning.

Limited NIC coverage continues to be a problem, especially among those who are poor or live in rural areas, which means that those without a NIC must continue to turn to family and friends to register a SIM on their behalf. MNOs also report that the NIRA API is regularly down and mismatches occur frequently, with some representatives estimating a 10 per cent failure rate. Stakeholders insist that the national registry needs to be better funded and resourced if the process is to be fully operational and meet the requirements expected by law enforcement agencies. The current biometric validation process also continues to impact MNOs' operational costs, as they must employ full time staff to check the data they collect and quickly verify this against the card details. Biometric verification also places a significant burden on the MNO in terms of network capacity and storage; 64-bit images are data heavy and this raises particular issues when uploading outside of the main urban environments.

Interestingly, representatives from two MNOs reported that they currently use paper forms for SIM registration as this allows them to capture the customer's signature, fulfilling the KYC for mobile financial services. Both MNOs then capture and store a digital copy of the form, the identity card and the biometrics of the subscriber. This amounts to a considerable amount of data and server capacity. MNOs would like for the electronic SIM registration process to meet the KYC requirements for the provision of mobile financial services, and there is an expectation that when the National Integration Plan comes into force and services are accessed through a digital signature, the KYC compliance process will be considerably less burdensome on MNOs.

CASE STUDY 5

Senegal

In October 2016, the Senegalese government started a national identity programme to move all citizens to a biometric identity card managed by La Direction de l'automatisation du fichier (DAF). The card contains two numbers – the individual's previous identity number and the new card number, plus biometric data (fingerprints). The card can be used for public services, including voting, healthcare, tax and passport, as well as free movement within ECOWAS, a community of 15 states in West Africa. By October 2017, coverage of the new identity card was at 72 per cent,[23] but over four million citizens were still not registered.

[23] See: https://globalfindex.worldbank.org

In 2007, MNOs were required by the ARTP (Regulation Authority for Telecommunications and Post) to validate the address and identity of all new using their identity card, and then store these details. At the time, there was no limit on the number of SIMs per person, which led to multiple instances of fraud. In 2013, at the request of external law enforcement, the government convened ARTP and the MNOs to discuss a technical solution for real-time identity validation.

From 2013 to late 2015, different approaches for the Capture and Validate system were considered, including the use of biometrics. MNOs pushed back on the use of biometrics, however, believing this system would be too costly when weighed against the level of security the government required. **Close collaboration between the government, regulator and MNOs ensured that the agreed approach – using biodata only – could be met by both MNOs and the national identity authority, and the presence of a dominant single operator has led to negotiations that balance government requirements for security with the commercial interests of MNOs.** With no pressing security needs, a considerable amount of time – just under three years – was allocated for planning, development and testing the new system. The national registry was well established and had sufficient time to build up its capacity to cope with the demand for real-time verifications required from MNOs.

In 2016, the ARTP directed that all MNOs had nine months to register all their customer SIM cards and validate their identities against the DAF database. MNOs were responsible for developing the integration with DAF database, and each developed their own proprietary system, with one operator developing its own internal verification system in order to provide a secondary check on their retail network.

The ARTP and MNOs shared the costs of communicating with the population that they had to re-register their SIMs in person. By November 2016, operators were required to deactivate any SIM cards that were not registered. One operator reported losing approximately 6 per cent of active SIMs, but the noted that the cancellation of these lines produced significant savings. The registration process is now fully digitised and does not place much of a burden on the network. However, the current registration process does not fulfil the KYC requirements for mobile financial services, as these require a separate application.

Key Learnings

Capture and Validate Implementation

The experiences of MNOs across the 11 research countries show that when implementing a new registration system, there are various factors that all governments, regulators and MNOs need to consider. The manner in which these factors are planned for and addressed can either facilitate the implementation and relieve some of the impact on MNOs, or vice versa. Across all countries, the following key learnings emerged:

Cross-Sector Collaboration and Consultation:

When Capture and Validate systems are implemented through cross-sector collaboration and with strong backing and support from government, a wide range of technical, procedural, legal, societal, financial and commercial challenges can be overcome effectively. Working closely at the outset of re-registration drives, setting shared objectives, and providing a clear rationale for implementing the new system will also help to engage and motivate MNOs. In Senegal, the impact of the new Capture and Validate system on MNOs was minimal, as consultations continued for two years until an agreement was reached that balanced government requirements for security with the commercial interests of MNOs. Meanwhile, the creation of a core project team led by the regulator worked well to direct the project and facilitate negotiations in Bangladesh and Pakistan. In Bangladesh, the Director General of the regulator led the project alongside the head of AMTOB, the organisation representing the MNOs. This team, in conjunction with MNO management, devised the overall strategy, planned the implementation and helped to ensure the MNOs' voices were heard by government. In Pakistan, the regulator played an important role lobbying government helping to reduce NADRA's fees and getting acceptance that MNO could make use of the identity data they already held.

Government Incentives and Support:

Governments supported MNOs in several of the research countries by delivering nationwide communications campaigns that were designed to encourage consumers to re-register their SIMs. Other government incentives, however, were less forthcoming. Local stakeholders often felt that the government could do more to support these programmes, especially in circumstances where the overriding objective was to improve national security. MNOs suggested a number of ways financial support could have helped them better navigate the implementation of these systems, including a reduction in SIM tax for the period of re-registration; receiving a contribution from government funds earmarked for social purposes; or a relaxation of any verification fees. In Pakistan, MNOs won a small concession and verification fees were reduced over the re-registration period. In Peru, no concessions were won over the re-registration period but, in 2018, the government acknowledged that SIM registration does have a public purpose and (temporarily) absorbed the fees.

Industry Collaboration:

Collaboration between MNOs can offer significant benefits during the implementation phase, including economies of scale in device procurement, faster technical integration through knowledge sharing, and a reduction in business downtime through more integrated customer activation. Negotiating with government as a single united team will also be more effective than engaging as individual entities. Collaboration is not necessarily easy, however, as SIM re-registration mandates can be seen by some organisations as an opportunity to gain a competitive advantage. In Bangladesh and Pakistan, there was a valid concern that the re-registration process would favour operators with more resources and a larger retail network, as this would enable them to reach the widest number of subscribers. However, evidence from the five focus countries suggests that where there are two or more MNOs with similar market share, 'going at it alone' does not confer any advantages in terms of customer acquisition.

Project Planning & Timelines:

With the exception of Senegal, shortened timelines and incomplete project planning caused major problems for MNOs. Hardware procurement decisions require time for testing, particularly in an environment where thousands of devices or scanners will be rolled out. In Pakistan, lack of testing time, particularly outside of the cities, led to procurement of multiple devices and increased costs. In Uganda and Peru, procurement was initially controlled by the regulator and national identity registry. This approach resulted in ongoing technical problems and left MNOs with no time to develop and test their own equipment. Stakeholder interviews suggest there would be a preference for open market tenders with longer lead times for testing. In Peru, one MNO estimated that 80 per cent of new SIM sales were affected in the first month of their registration programme and 15 per cent of sales overall during the registration period due to technical problems.

Many MNOs also underestimated the amount of time and effort required to train staff on how to implement the new Capture and Validate processes, and to motivate customers to re-register. In Pakistan and Uganda, for instance, MNOs 'shut down' many of their business operations for nearly three months as employees were sent to all areas of the country to support customer activations. Despite these efforts, large numbers of customers did not register in time, and their SIM cards were deactivated. Ensuring appropriate timeframes and alternative processes are in place will also minimise the risk of excluding those without the required documents.

National Identification Coverage and Database Capacity:

To help prevent disruptions, citizens need access to the requisite national identity documents, and the national registry must contain up-to-date and accurate information. In Uganda, re-registration activities were conducted when only 70 per cent of the population had access to a national identity card, which means that a significant number of subscribers were forced to use another person's identity to acquire a SIM. MNOs in Bangladesh, on the other hand, were permitted to register customers using alternative identity documents, so long as they produced the NID card within six months of registration; this was an effective strategy resulting in just 14 million deactivations out of a total of 131 million SIM subscriptions.

In all countries, the national identity registries struggled to cope with the volume of verifications requested by MNOs, resulting in regular downtime and loss of sales revenue. Data mismatches were also common, particularly when validating customers' biometrics. In Peru, this increased the cost to MNOs as they are charged for every verification attempt and no alternative process is permitted. MNOs would like to see governments invest in the national registry so it has the resources and capacity to meet the needs of subscribers and MNOs.

Weighing the Need for Biometrics vs Biodata:

Extensive consultations took place in Bangladesh and Pakistan on the subject of biometric verification. Although MNOs were initially against the use of biometrics due to the high upfront costs, all parties eventually came to a consensus that biometrics were the most viable route due to the prevalence of fake identities in the market. There is less consensus among stakeholders in Peru concerning the value of implementing a biometric verification system (BVS). Some noted that the BVS has raised the cost of SIM registration, and also had the potential to exclude some segments of the population whose fingerprints may be worn or harder to scan and validate. There is a preference for KYC processes that do not require a customer to be physically present, and look at KYC processes used by banks as worth exploration.

Leveraging Know-Your-Customer Processes:

If MNOs are to leverage the new system for digital identification, they need regulators from other sectors to agree that the KYC processes are satisfied through this new SIM verification process. This was achieved in Pakistan, where the Financial and Telecoms regulators agreed that that KYC would be satisfied for a mobile wallet, thereby having an immediate positive effect on the financial inclusion agenda. Similarly, in Uganda two MNOs decided to combine the application for SIM registration and financial services on the same application form (in effect, the addition of a signature). This has added considerable time, resource and cost to the process – MNOs conduct their own validation in addition to the national registry – but it means customers do not have to sign up separately for a mobile wallet account. Stakeholders in Bangladesh, meanwhile, noted that Capture and Validate processes have given the mobile number as much credibility as an ID validation tool as the actual NID. Banks and other financial services providers recognise this, and have voiced interest in linking into CBVMP and using SIMs as one element of their KYC processes.

Benefits to MNOs

Across all five of the focus countries, there was consensus amongst stakeholders that the new Capture and Validate system had delivered a number of important benefits. This includes:

- **Improved Database Management:**
  MNO representatives agreed that the verified registration information provided by Capture and Validate systems has resulted in cleaner customer databases, and that these can help operators manage their customer relationships more effectively and offer more appropriate products and services. However, customers' ability to register multiple SIMs against a single identity document and other cultural factors means that profiling the actual mobile user, rather than just the registered user, remains difficult. In Pakistan, as in many other countries, many SIMs are registered by the (typically male) head of household, who passes the SIMs on to family members. In this context, individual customer profiling becomes more challenging and restricts MNOs' ability to generate incremental revenue through personalised services, especially those targeted at women.

- **Improved Tracking and Customer Authentication:**
  In Bangladesh, Pakistan and Uganda, new platforms have been developed by the telecommunications regulator to provide greater visibility over a mobile subscriber's identity and mobile activity. These new digital platforms contain valuable data that could be used to validate an individual's identity, and there was interest among stakeholders to use these as additional KYC authentication services to improve access to financial and government services. The Pakistan Mobile Database currently provides subscriber verification services to individuals, banks and government departments, including the tax authority and financial regulator. In Bangladesh, there is interest from banks to use the Central Biometric Verification Monitoring Programme platform as part of the KYC verification process. MNOs in Peru voiced a reluctance to test new ways of leveraging identity data to market new services to customers without permission, due to strict data privacy regulations.

Streamlined Process and Improved Customer Experience:

In Senegal and Bangladesh, the move from paper-based to digital SIM registration applications has improved the speed and efficiency of the KYC process, and has reduced MNO costs related to scanning, uploading heavy images, and storing both soft and hardcopy registration documents. Capture and Validate registration processes have also improved the customer on-boarding experience. Jio, an MNO in India, has seen phenomenal growth in user acquisition using the Aadhaar database for verification, with the on-boarding process taking just 30 minutes. Interviewees in India described the SIM registration process before Aadhaar as 'confusing and burdensome'; customers were required to bring various documents to complete registration and SIM activation could take up to 72 hours.

Reduction in Small-Time Criminality:

The majority of interviewees noted that the Capture and Validate system had greatly enhanced MNOs' ability to trace SIMs back to a unique individual (as well as to a specific vendor) – a key security objective for government and law enforcement. Some MNO and government representatives anecdotally reported a reduction in the level of crime, in particular what was referred to as 'small-time' criminality. While no hard empirical and published data was available to support these assertions, stakeholders pointed to a reduction in consumer complaints and lower numbers of investigations into particular types of crimes. In Pakistan, Bangladesh and Uganda, hoax calls and mobile money fraud has reportedly been reduced (anecdotally, up to 80 per cent in Uganda and Bangladesh) and in Peru, the regulator reported a decline in extortion calls via mobile.

Rationalising the retail network:

Capture and Validate systems have required many MNOs to rethink their retail network strategy, after new legislations mandated that they complete all new SIM registrations in dedicated MNO stores or through selected franchise outlets. In Uganda, this 'bricks and mortar' strategy was mandated by the regulator and brought into effect quite quickly; in Bangladesh and Pakistan, a phased approach was allowed given the size of the retail network and the need to equip each store with scanners and devices. The impact of these changes in each country has been positive overall, resulting in more transparent and accountable processes, strengthened back-end systems and better trained sales channels.

Economic Impact on MNOs

The benefits of Capture and Validate systems, as outlined in the previous section, can be costly for MNOs. In each of the focus countries, operators were expected to cover all costs associated with implementing the new system and most saw reductions in their customer base – for some operators, this reduction was significant. MNO representatives participating in this research were not always able to provide detailed information related to the total investments made or ongoing operational expenditure (which is updated regularly and difficult to extrapolate). Therefore, the figures below are indicative estimates of the investment required by a single operator in these countries with a retail network and subscriber base as specified.

- The amount of capital investment made by MNOs – for example to purchase scanners, other devices, and servers – varied according to the size of the organisation's retail network, subscriber base and whether biometrics or biodata was required. MNOs in Peru, Bangladesh, Pakistan and Uganda were all required to invest in registration devices and biometrics scanners; in Senegal alone, MNOs were only required to purchase devices that helped validate biodata. Operational expenditure depends largely on training requirements, data capture and storage needs (text and/or images) and verification fees. Notably, the operational costs after the new registration system have reportedly decreased in most countries.

	Peru	Bangladesh	Pakistan	Uganda	Senegal
Retail Outlets	8,000	25,000	50,000	12,000	3,000
Unique Subscriber Base	15m	40m	40m	11m	9m
Average Revenue Per Customer (ARPU)	$3	$2	$2	$2	$2
Total Investment per Operator (Estimated)	$5-10 million	$15-25 million	$25-35 million	$5-10 million	<$1 million
Cost Allocations					
Scanners, devices, servers, retailer training, customer activation	35%	65%	50%	80%	70%
Data Platform	5%	5%	5%	10%	10%
Verification Fees	60%	5%	10%		
SIM Tax		25%	35%		
Internal Verification				10%	20%
Increase/Decrease in costs since new system in place					
Administration/Transaction costs	Increase	Decrease	Decrease	Same	Decrease
Compliance costs	Decrease	Decrease	Decrease	Increase	Decrease
Penalties	Decrease	Decrease	Decrease	Same	Decrease

Implementation of the new Capture and Validate system resulted in customer losses to most, if not all, operators. These were largely expected, but perhaps not to the extent seen in Pakistan and Uganda, where there was a large amount of SIM redundancy as well as deactivations. In Pakistan, operators reported losses between 10 and 20 per cent; in Uganda loses of around 13 per cent were experienced. Re-registration activities did tend to disproportionately benefit MNOs with the largest market share, but perhaps not to the extent that the smaller MNOs feared, particularly in Bangladesh.

Current and Future Opportunities

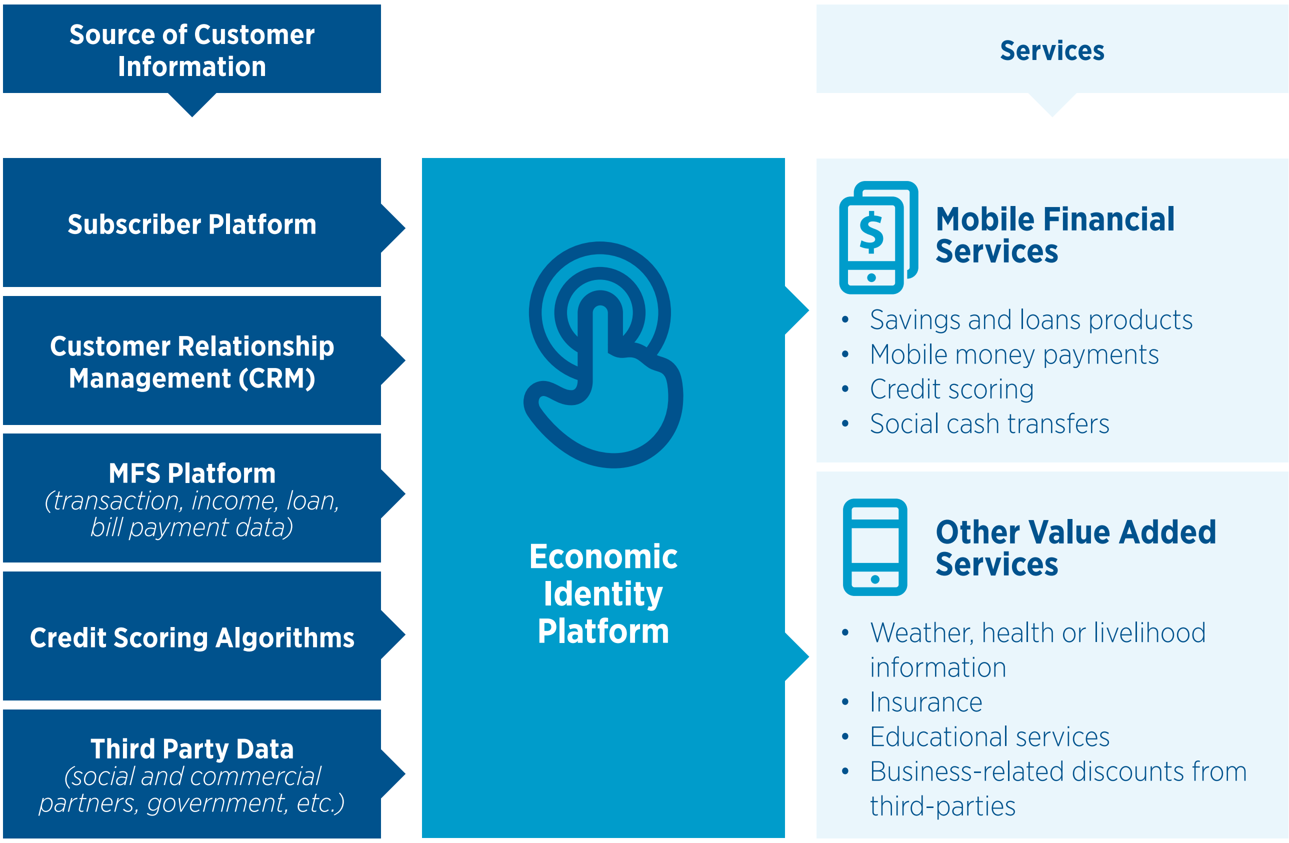
Currently, with the exception of Pakistan, MNO representatives engaged through the research indicated that their organisations are not currently leveraging Capture and Validate identification processes, or their improved customer databases, to offer new identity-linked services to customers. However, all MNOs voiced interest in working with the GSMA and other partners to explore how new business or partnership models could help them achieve this, and there is also a clear appetite to learn from 'best practice' approaches used in other countries.

In Pakistan, MNOs have already embraced opportunities to leverage KYC processes to improve access to public and private sector services. During the national SIM re-registration drive, an agreement was reached between the Financial Regulator and the Telecoms Regulator that the KYC criteria for opening a mobile wallet would be satisfied through the new Capture and Validate process. This has had a very positive impact to the financial inclusion agenda; as documented by the GSMA,[24] this agreement allowed MNOs to open new mobile money wallets for customers at the same moment their SIMs were being re-registered. The value that mobile money services can bring to the financially excluded, and women in particular, is clear; through partnerships with the Benazir Income Support Programme (BISP) and CARE International, Telenor's Easypaisa service has helped overcome cultural and logistical barriers by bringing financial services to local corner shops, enabling women to register and receive their cash disbursements without having to travel to a bank. Other services offered in Pakistan that require identity authentication include health cards (health insurance and information offered by Zong) and Internally Displaced Person cards to support refugee relief.

The GSMA Digital Identity programme has established that MNOs with access to verifiable customer data are well-positioned to champion the development of reliable 'economic identities'.[25] In this case, the term 'economic identity' is used to describe a form of functional identity, which tend to evolve out of a single use-case (similar to voter IDs, health records, or bank cards) with the potential for use across sectors. MNOs can help establish economic identities by collecting, sharing and collating a wide range of customer data from their own databases, as well as from external sources. These digital profiles are built on the understanding that MNOs, formal financial institutions and other service providers would be better able, and more willing, to extend services to customers if they were able to validate their official identity, as well as their shifting, dynamic needs and economic situation; this could be done by authenticating relevant credentials such as their income, occupation, gender, mobile transactional histories, credit histories, approximate location and eligibility for government services. Ownership of both official and economic identities would therefore provide customers with greater access to mobile money services, government subsidies, targeted information, formal financial products, and other valuable services that improve their livelihoods and well-being.

[24] GSMA (2017) 'Understanding the Identity Gender Gap: Insights and opportunities for mobile operators to help close the divide'
[25] GSMA (2018) 'Digital Identity for Smallholder Farmers: Insights from Sri Lanka'

Developing an Economic Identity



Source of Customer Information

- Subscriber Platform
- Customer Relationship Management (CRM)
- MFS Platform *(transaction, income, loan, bill payment data)*
- Credit Scoring Algorithms
- Third Party Data *(social and commercial partners, government, etc.)*

Economic Identity Platform

Services

Mobile Financial Services

- Savings and loans products
- Mobile money payments
- Credit scoring
- Social cash transfers

Other Value Added Services

- Weather, health or livelihood information
- Insurance
- Educational services
- Business-related discounts from third-parties

Many MNOs in the research countries were engaging in the sponsorship of new businesses, generally through tech hubs which develop new applications in sectors such as transport, microfinance, health and agriculture. MTN Uganda has opened up its mobile money service via an API for developers, while Sonatel in Senegal supports a range of applications, such as Firefly, a community transport service, and MaTontine, a mobile-based automated microfinance platform. In March 2019, GSMA conducted research in urban Nigeria to explore how MNOs could help catalyse the growth of smaller-scale enterprises through the provision of identity-linked services. Discussions with business owners confirmed that they feel marginalised by many formal financial institutions, highlighting a real need for an identity platform that gives entrepreneurs more credibility among service providers and better access to the resources they need to grow their businesses. With this in mind, developing a data-driven 'economic identity' – leveraging data sources from MNOs and other partners – could be an initial first step, likely using a mobile financial service package as the 'anchor' product. These services were of significant interest to small-scale businesses, and the wider data model of interest to MNOs and other service providers. Business owners were also keen to share their identity information if it could help them become more productive, particularly with suppliers, distributors, and customers.

There is also interest among MNOs to explore how Capture and Validate systems can be leveraged to open access to services provided by other institutions, such as government or financial service providers, with higher-tier KYC requirements. For this to take place, regulators will need to agree that the identification of the subscriber has been validated in such a way that it satisfies the KYC criteria for that sector. In Senegal, for instance, biodata verification is not considered to be sufficient for accessing mobile financial services (MFS), which means that subscribers must apply separately for in order to access these services. In Uganda, MNOs are allowed to supplement the standard SIM registration process so that the subscriber also becomes eligible for opening a mobile wallet. In Bangladesh, the new SIM registration process has begun to establish the idea of 'my SIM is my identity', but the industry has been, so far, blocked from access to MFS. The situation does look to be progressing, however. According to interviewees, banks and other financial service providers recognise the high level of assurance provided by the SIM registration process and have started to explore how to link into the central database (CBVMP) as an authenticating factor. MNOs have also started to make inroad into MFS by partnering with banks and insurance companies, offering their network as access points.

Finally, an estimated one billion people do not have access to official forms of identification,[26] and the most significant 'identity gaps' are found in the same locations where mobile connectivity and mobile agent networks continue to scale. This indicates that MNOs are well-placed to provide national governments and other ecosystem players with the opportunity to leapfrog inefficient, paper-based identity registration systems and offer more inclusive methods of providing unique identities to the underserved. In Nigeria, the National Identity Management Commission has published an advertisement inviting private sector entities to formally express their interest to become licensed partners to support citizen enrolment into the new digital ID programme.[27] This policy paves the way for MNOs in Nigeria – and hopefully elsewhere – to play a much more hands-on role in accelerating the digital identity ecosystem and offering additional services to their (newly identified) customers.

Conclusion

This report has confirmed that nine out of the 11 countries selected for this research operate a 'Capture and Validate' SIM registration system. This approach, which can be delivered virtually (via short-code or interactive voice response) or by the subscriber submitting their details in person, provides a number of benefits to MNOs. These include a more streamlined process resulting in a better on-boarding experience for consumers, and a reduction in administration, transaction and compliance costs.

In some countries, implementing the change to a Capture and Validate system has been relatively straightforward and has had a minimal impact on MNOs and their operations. In others, where the implementation timeframe was short and the national registry lacked sufficient coverage, the impact on MNOs and customers has been significant. The impact on MNOs was felt particularly strongly in Uganda and Pakistan, where up to 30 per cent of the population lacked access to a national identity document at the time of re-registration, and the system had to be implemented in a very short period of time. In all situations, government support (which might include financial incentives or mass communications campaigns) and industry-wide collaboration can help mitigate the impact on MNOs.

In all countries, the national identity registries struggled to cope with the volume of verifications requested by MNOs, resulting in regular downtime and the potential loss of sales revenue. Data mismatches were – and in some cases remain – common, particularly when validating customers' biometric details; this is a particularly costly challenge for MNOs in Peru, who are charged for every verification attempt. MNOs would like to see governments invest more in the national registry so that it has the capacity to meet the needs of subscribers and MNOs.

Five countries have moved to a system where the subscriber must validate themselves and their identity card using a combination of biometrics and biodata. The additional layer of biometric verification has improved accountability within the SIM registration systems, which are the least likely to suffer from identity fraud or compliance abuse. However, some stakeholders noted that biometric systems raise both implementation and operational costs for MNOs, and also have the potential to exclude some segments of the population whose fingerprints may be worn or harder to scan and validate. In countries where Capture and Validate systems are likely to be mandated, it is important that MNOs work proactively with government to help weigh the benefits of biometric versus biodata systems, and ensure that a balance is struck between the government's security requirements and the commercial interests of MNOs.

The research has supported GSMA's assertion that Capture and Validate processes give the highest level of assurance that the registered individual 'is who they claim to be', which mitigates the incidence of fraud and offers new opportunities for mobile to be used as a digital identity when accessing value added services. MNOs in Pakistan have set the precedent for realising these opportunities. Harmonising SIM registration requirements with KYC requirements for accessing MFS has meant

MNOs are now delivering financial services to large parts of the population who were previously unbanked. This has generated incremental revenue for MNOs and opened up the potential for a range of new products and services. In other countries, where regulatory harmonisation has not taken place, MNOs have not yet been able to take advantage of these opportunities, though MNOs in Bangladesh are making progress in getting access to mobile financial services. As countries move towards greater accountability in SIM registration processes, particularly in Africa, MNOs could see the investment required to implement a Capture and Validate process as a means to opening up new revenue-generating services, rather than simply a financial burden imposed by government to enhance security.

Only 11 years remain to meet the 2030 United Nations' Sustainable Development Goals (SDGs), and in particular SDG 16.9 which aims to provide a 'legal identity for all'. There is a clear need for governments, the development community, and the mobile industry to work together to address the barriers that prevent millions of individuals from accessing official proof of identity and benefitting from life-enhancing mobile services that are registered in their own name. The GSMA Digital Identity team is committed to supporting focused research and advocacy efforts, coupled with in-country demonstration projects, to create more enabling environments where the needs of underserved groups are better catered for. This involves advocating for and exploring various unique roles that its mobile network operator members can play in bringing the benefits of digital identity to the poorest and hardest to reach individuals around the world. If you are a GSMA member, policymaker or other organisation seeking to pursue digital identity solutions for the urban poor and other underserved populations, please contact the Digital Identity team at digitalidentity@gsma.com.

Appendix 1
Additional Country Case Studies

Ecuador

Population:
16 million

Smartphone Penetration:
54%

Mobile Penetration (unique subscribers):
69%

Subscription:
77% prepaid; 23% contract

The Cedula de Identidad is the official national identification credential in Ecuador, issued by the Civil Registry. It includes the biometric data of each cardholder. Citizens can use their national identity card to travel within the country, register for a passport and for voting. Ecuadorians of all ages are eligible to obtain a Cedula de Identidad at cost of $5. Ecuador has a comprehensive identification system in place with 99 per cent of the population registered.[28]

In 2011, the Telecommunications Regulation and Control Agency (CONATEL) made SIM registration mandatory in Ecuador. Citizens can use their identity or other official documents for registration and can activate the SIM calling the operator automated service. The operator validates the identity against the Ecuadorian Civil Registry in real-time. MNOs are obliged to capture the full name, address, identification number and the year of issue; they must also link the identity details to the user's handset IMEI number and store the details for five years. Since 2012, all citizens have been required to register their IMEI number with Arcotel (the regulator), which hold an IMEI blacklist of all lost and stolen devices. Both the SIM and the IMEI number must be registered against a single identity to be validated and this data is stored by the MNO.

MNOs were responsible for developing the system that automatically records the identity number and connects to the civil registry for validation. In addition, MNOs had to invest in largescale communications to ensure everyone validated their SIM card. This was supported by the Minister of Telecommunications, who declared that, if people do not register, the lines and the devices could be blocked even outside the country (agreements for cooperation were under negotiation with Colombia and Peru).

Overall, MNO representatives think the new system has been positive and brought about some benefits: a clean database has meant better targeting of promotions and new products; phone theft has been reduced (anecdotally by 50 per cent); and national security has been improved overall. However, there is some concern about the introduction of biometrics, which they believe add more to costs and operational inefficiencies than it does to security. No new services have been developed on the back of this identity validation process so far.

[28] See: https://globalfindex.worldbank.org

India

Population:
1.36 billion

Smartphone Penetration:
46%

Mobile Penetration (unique subscribers):
55%

Subscription:
93% prepaid; 7% contract

In 2010, India launched a programme called Aadhaar, the world's most ambitious national identity project. The Aadhaar is a unique 12-digit number issued by the Unique Identity Authority of India (UIDAI), available to all residents at no cost and valid for life.[29] Among other things, the Aadhaar number enables residents to open a bank account, get a driver's license and apply for a passport. As of December 2017, the UIDAI have registered more than 1.2 billion[30] people on the database – approximately 89 per cent of the population.

SIM registration has been mandatory in India since 2005 but, until 2017, it was seen as inefficient and time-consuming. Customers had to bring various documents and the SIM might not be activated for up to 72 hours. In 2017, the Department of Telecommunications (DoT) issued a directive that all new and existing SIM cards must be verified against the Aadhaar registry. Mobile operators needed to comply in full by 6 February 2018.[31]

All mobile subscribers needed to visit a MNO retailer to complete biometric SIM registration. New customers must complete a Customer Acquisition Form (CAF). In addition to sharing their Aadhaar number, customers also have to have their fingerprints and/or iris scanned using a biometric reader. These details are then validated against the UIDAI database via an online portal.[32] If the identity is confirmed, the MNO agent requests UIDAI to send a One Time Password (OTP) to the customer's mobile number. The process is fully digital and a SIM can be activated in 30 minutes. Each customer can register for a maximum of nine SIM cards.

On 26 October 2018, the Supreme Court stipulated that it was no longer a requirement of the operators to validate users' identity using Aadhaar.[33] MNOs were instructed to accept other documents, such as a driving licence, passport and voter identity card.[34] Only new SIMs would require this validation and all existing SIMs based on Aadhaar e-KYC would be safe and not discontinued.[35] MNOs responded by suggesting a CAF to be embedded with live photographs and scanned image of Proof of Identity or Proof of Address ensuring it stayed a completely digitised process. There has been no resolution to date.

Timelines for re-registration were tight but MNOs did benefit from some cost sharing of biometric devices as customers could re-register at any operator outlet. No government incentives were given. MNOs are very positive about the SIM re-registration system against Aadhar and believe it has realised a number of benefits:

- A clean database
- Reduction in fraud (the previous paper-based system was open to abuse with duplicate / fake identities registering for additional SIMs)
- A more streamlined process – no need to process and verify multiple documents – against Aadhaar it is fully digital and validation is in real-time.
- The system has facilitated on-boarding new customers. Jio – a new operator – has acquired 218 million new customers (end of 2018) primarily from marginalised communities where residents previously lacked identity.

MNOs are concerned that the new ruling from the Supreme Court will mean a return to the old system, which will increase costs from ₹15 per person—the current cost of e-KYC verification—to ₹100 per person for a physical KYC. The offline process could also take 24-36 hours.[36] MNOs are very cautious about leveraging customer data for promoting new services and products due to recent changes to privacy regulation.

[29] Wharton Fintech (2017) 'Your guide to UPI—the world's most advanced payments system'.
[30] See: https://uidai.gov.in/aadhaar_dashboard/
[31] According to Government of India, see: dot.gov.inhttp://dot.gov.in/sites/default/files/Re-verification%20instructions%2023.03.2017.pdf?download=1
[32] Ibid
[33] Ibid
[34] The Economic Times (2018). 'Aadhaar not mandatory for mobile SIMs, you can submit other documents too'.
[35] NDTV (2018) 'Centre Explains How Top Court's Aadhaar Verdict Impacts Mobile Users'.
[36] LiveMint (2018) 'How telecom companies will verify new users without Aadhaar'.

Ghana

Population:
30 million

Smartphone Penetration:
50%

Mobile Penetration (unique subscribers):
54% [37]

Subscription:
98% prepaid[38]; 2% contract

In 2006, the National Identification Authority (NIA) was set up to implement a national registration programme and issue national identity cards.[39] In 2008, NIA was given authority to collect personal and biometric data and ensure the protection of privacy and personal information.[40] A resident of Ghana aged 15 and above must obtain a national identity. Each card is valid for 10 years and contains a personal identity number, personal details and biometrics in a machine-readable 2D-barcode.

The objective of the NIA was to harmonize all identity systems and oversee a national database, communications networks, security and card production systems.[41] However, although 11 million citizens were registered in 2009, the programme has since disintegrated with the cards being rejected by some banks and state institutions.[42] Today, no single government database based on a single identity exists yet in Ghana, rather there a number of different databases which provide validation for different services, such as social welfare, health insurance, electoral services and driving licences.

The National Communications Authority (NCA) is responsible for regulating the mobile industry the National Identity Register regulations (2012) state that an identity card is mandatory for SIM registration.[43] Enforcement, however, has varied over the past six years, with the NCA issuing a number of directives to MNOs to register their customers' SIM cards with varying degrees of success. Currently, customers can register a SIM with different identity certificates in dedicated operator stores as well as via street vendors (there are c.13,000 street vendors around the country). All SIM vendors are required to capture the name, address, identity document and MSISDN and store these – either on paper or electronically. MNOs are required to collect and store these forms, which can be accessed on request by law enforcement agencies and the courts.

The requirement to collect and store paper registration forms is considered expensive and serving little purpose in terms of traceability and supporting law enforcement. MNOs have begun to develop capabilities to validate identity against other databases, such as voter identity and national health insurance cards, and anticipate that government will mandate identity validation at some point.

MNOs see significant opportunities in developing a robust identity framework, particularly for mobile financial services and e-commerce. MNOs are fully behind implementing robust KYC processes for SIM registration as this could facilitate access. Currently, a customer is required to enter two distinct records for mobile money and SIM registration. Views differ on whether validation against a single national database or a more open identity framework will work best. The former option has given rise to a lot of discussion around data privacy and protection. The latter option would involve greater interoperability between databases but seems to some, given the nascent state of the national identity programme, the option that is most workable.

[37] GSMAi
[38] http://prepaid-data-sim-card.wikia.com/wiki/Ghana
[39] See: Ghana National Identification Authority Act, 2006 Act 707
[40] ibid
[41] See: https://www.nia.gov.gh/faq.html
[42] GhanaWeb (2018) 'National ID cards ready, to be issued from May 28 – NIA'
[43] NATIONAL IDENTITY REGISTER REGULATIONS, 2012

Indonesia

Population:
268 million

Smartphone Penetration:
90%

Mobile Penetration (unique subscribers):
75% [44]

Subscription:
96% prepaid; 4% contract

All Indonesians over the age of 17 must hold a Kartu Tanda Penduduk (KTP), the Indonesian identity card. The card contains a unique number (NIK) consisting of 16 digits[45] and recent legislation has stipulated that this is now a lifetime card. The KTP is issued, and all data held, by the Population and Registration Service Agency (DUCKAPIL) under the Ministry of Home Affairs. In addition to the KTP, each family is required to have a Kartu Keluarga (KK), a card that holds all the details of family members, managed by DISDUKCAPIL (local registry).

In 2011, the Ministry of Home Affairs launched a nationwide programme to issue an electronic identity card (e-KTP) to all Indonesians. The e-KTP contains multi-model biometrics (fingerprints, face and iris)[46] and is valid for life. The intention is that citizens will be able to access services with just one card. By 2013, the biometrics details of 173 million people were registered with DUCKAPIL.[47] According to an Interior minister who was interviewed for this project, 97 per cent of the population in 2019 is registered in the national civil registry database.

Until 2017, any citizen wanting a SIM card would text in their identity details via the SMS short code 4444. The data would be held by the MNO and the SIM would be activated. The MNO was obliged to submit a report on customer data every three months to the Indonesia Telecommunication Regulatory Authority (BRTI) and a subscriber could register 10+ card.[48]

In October 2017, the Ministry of Communication and Information Technology (MOCIT) via the regulator (KOMINFO) required that all SIM cards (new and current) must be validated against the DUKCAPIL database using a combination of the NIK and Kartu Keluarga. The customer must input a keyword, identity Number and family card number via a short code to 4444. MNOs pass the data to DUKCAPIL and they validate the NIK & Family card data in real-time. MNOs send the MSISDN number to DUKCAPIL during the validation process in order to map each MSISDN registered to an identity. Both MOCIT / KOMINFO and DUKCAPIL have access to the registration data. The process is the same for new registrations and re-registration of current cards, just the keyword is different. The current limit for SIMs is 3 per operator per identity if registering via the short code. If more SIMs are required, e.g. for M2M (data), then the subscriber must register in store.

All mobile subscribers were required to re-register their SIM by 28 February 2018 or suffer service suspension. On 28 February, over 200 million SIM were re-registered. In March, KEMKOMINFOR blocked 100 million unregistered prepaid SIM cards with activity restored if accounts registered by 1 May 2018.[49] By April 2018, 245 million SIMs were registered.

[44] GSMAi
[45] Indonesian Government directive, 2006
[46] Population and Development Review (2017) 'Identity Systems and Civil Registration in Asia'
[47] Planet Biometrics (2012) 'Indonesia ID project makes stunning progress'
[48] See: https://jdih.kominfo.go.id
[49] ibid

Malaysia

Population:
31 million

Smartphone penetration:
95%

Mobile Penetration (unique subscribers):
80%

Subscription:
66% prepaid, 34% contract

In September 2001, the National Registration Department of Malaysia (NRD) introduced MyKad, the national identity card, making it compulsory[50] for all citizens aged 12 and above. The card is based on a unique series of digits and the NRD is the sole authority in charge of issuing the NRIC numbers.[51] The advanced chip and biometric technology allow its users to access government services, including driving, travel, healthcare, e-cash (a reloadable cash purse accepted at government agencies, petrol stations), public transport. The card can also double up as an ATM card at designated banks[52] and a loyalty card at several retail outlets.[53]

In 2006, the Malaysian Communications and Multimedia Commission issued guidelines that all SIM cards should be registered. In 2013, these guidelines were updated, directing that a subscriber's identity should also be verified. At the time, subscribers could present their identity in person at the MNO store or could provide their identity number via USSD.

In 2016, MCMC directed that all registrations should be auto populated by a card reader or via biometrics and manual input was no longer permitted. Citizens have to present their MyKad in person and register at a service provider outlet. MNOs were required to procure MyKad readers and/or Optical Character Readers and store the details on the card, including name, identity number and address. All the costs for hardware and registration applications were to be borne by the MNOs. MNOs and Government undertook nationwide communications to alert consumers that they needed to bring their card for registration for a new SIM.

MCMC has asked that MNOs provide MCMC with the identity numbers attached to the new SIMs so they can be validated against the national identity registry. These are validated in batches and, where there are inconsistencies, MNOs must re-validate with the subscriber or deactivate. Citizens can also purchase a SIM online if paying by a bank account as a bank account provides sufficient KYC details for SIM card validation. MNOs have mixed views over the effectiveness of the current system. Whilst they have benefitted from a clean-up of their database (c.80 per cent accuracy, reportedly) there are still opportunities for fraud and, with a five SIM limit per operator, MNOs still find it difficult to identify accurately each mobile user.

MNOs expect that real-time validation against the national registry is likely to come online in the next year or so. MNOs see a lot of value in validating the identities of all SIM subscribers – in terms of national security, reducing fraud and identification / profiling of customers. In particular, MNOs value the potential to assess a customer's credit rating and promote additional services through this identity verification process. There are some concerns that the move to a real-time verification system could be costly for MNOs and they would like other federated systems, such as those used in the US / UK, to be considered.

[50] See: http://www.jpn.gov.my
[51] See: http://research.omicsgroup.org
[52] PPC (2015) 'MyKad: Is Malaysia ahead of the game?'
[53] GSMA (2018) 'Digital identities: Advancing digital societies in Asia Pacific'

Thailand

Population:
69 million

Smartphone penetration:
92%

Mobile Penetration (unique subscribers):
86%

Subscription:
70% prepaid, 30% contract

In 2015, the Thai government implemented the smart identity card program with the aim of providing citizens with access to a wide range of public services via a single identity. The card contains biometric data (fingerprint + facial) and is mandatory for all citizens aged 7+. The Bureau of Registration Administration (BRA) is responsible for national identity cards[54] supported by the Ministry of ICT. According to the BRA, 97 per cent of the population is registered.[55]

In June 2014, following terrorist incidences involving unregistered SIM cards, the National Broadcasting and Telecommunications Commission (NBTC) made it mandatory for operators to register SIM cards on their networks. NBTC provided operators with a mobile application that captured the MSISDN and a picture of the subscriber's identity card. This data was uploaded to NBTC and the SIM then activated. NBTC sent the identity number and an image of the Thai identity card back to the operators. Registration was a nationwide exercise, which revealed that, out of the 90 million prepaid active SIM cards, only about six million had been registered.[56]

Operators were unable to capture subscribers' biodata and offer promotions using the NBTC application and so developed their own. These replicated the NBTC process but used a card reader to unpack the biodata contained on the card, i.e. first name, last name, address and date of birth. These applications were rolled out gradually to operators' dedicated stores. The vendor network – about 15,000 across the country – continued to use the NBTC system.

In late 2017, NBTC introduced biometrics, directing that a subscriber's facial picture should be captured and matched with the image on the identity card to validate the subscriber was also the identity cardholder. NBTC updated their application with image processing software that automatically compared the subscriber's face with the biometric data on the identity card. Operators updated their applications so that staff could compare the subscriber's image with the image on the card and validate manually. Once the biometric match is confirmed, and all the biodata data is captured by the operator and shared with NBTC, the SIM is registered and activated. From 2018, NBTC asked operators to report on the number of identities with more than five SIMs.

The impacts on MNOs include:

- Developing the proprietary application and training staff is seen as significant.
- The speed at which SIM sales take place has slowed which has impact on overall total sales.
- Collecting user biodata in operator centres has led to improved targeting for these customers
- However, large numbers of customers are still registered by vendors using the NBTC application, which provides no customer biodata. Operators still have to conduct CRM campaigns to capture this data
- Operators admit that the previous system was open to criminal activity and concede that the new system has tightened up security. Overall, operators argue that government has benefitted from the new SIM registration rather than operators.

[54] See: www.cdg.co.th
[55] See: https://globalfindex.worldbank.org
[56] Thailand Guru: 'Mobile Phone Number SIM Card Registration in Thailand'

Appendix 2: Research Methodology

The GSMA identified 16 countries that were thought to operate 'Capture and Validate' systems. Of these, 11 countries were selected to be part of this research: Bangladesh, Ecuador, Ghana, India, Indonesia, Malaysia, Pakistan, Peru, Senegal, Thailand and Uganda. The research was conducted in two phases:

Phase 1: Desk research

Desk-based research was conducted to provide a detailed overview of the key stakeholders, institutions, regulations, legislation, systems and processes that contribute to the C&V system in each of the following countries: Ecuador, Peru, Ghana, Senegal, Uganda, Bangladesh, India, Indonesia, Malaysia, Pakistan and Thailand. This included a review of all published material relating to SIM registration in the 11 countries, including reviewing published material in English, French, Bengali, Bahasa Indonesian and Spanish.

A total of 13 expert interviews with at least one MNO was conducted in each country. The expert/local knowledge was used to validate the available published information, which can often be incomplete or inconsistent. At a minimum one stakeholder interview was conducted in each country (by phone or skype).

A debriefing session was used to review the initial findings from the desk research and reach a final agreement on which five countries (and local stakeholders) would be targeted in Phase 2 of the project. The recommended countries included: Peru, Bangladesh, Pakistan, Uganda and Senegal.

Phase 2: In-country face to face research

Between January and March 2018, face-to-face discussions with MNOs, regulators and other stakeholders were held in each of the five selected countries:

- **Peru:** Telefonica, Claro, OSIPTEL
- **Bangladesh:** Robi, Grameenphone, Banglalink, Teletalk, Bangladesh Telecommunication Regulatory Commission, Association of Mobile Telecom Operators
- **Pakistan:** Telenor, Jazz, Zong, PTA
- **Uganda:** MTN, Africell, Sure, Uganda Communications Commission, National Information Technology Authority
- **Senegal:** Sonatel

The expert interviews allowed the researchers to collect more reliable data on the impact of these initiatives, develop a more rigorous analysis of the commercial benefits and costs associated with these processes, and develop recommendations for other MNOs based on lessons learned.

Our thanks to: Telefonica Ecuador; MTN Ghana; GSMA India; Ooredoo Indonesia; Yes and Celcom (Malaysia); True (Thailand); Robi, Grameenphone, Banglalink, Teletalk (Bangladesh); Bangladesh Telecommunication Regulatory Commission, Nurul Kabir (Association of Mobile Telecom Operators in Bangladesh); Major General Md. Emdaul Ul Bari (ex-Director General, BTRC); Telenor, Jazz and Zong (Pakistan); Pakistan Telecommunication Authority; Telefonica Peru, Claro (Peru); Sonatel (Senegal); MTN Uganda; Africell (Uganda); Uganda Communications Commission; National Information Technology Authority (Uganda).

gsma.com

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601