Commercially Sustainable Roles for Mobile Operators in Digital ID Ecosystems

Leveraging SIM registration and mobile money KYC (Know Your Customer) proof-of-identity compliance to accelerate digital inclusion

April 2021

Digital Identity

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators and nearly 400 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

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

Authors:
Christopher Lowe, GSMA Digital Identity
Yiannis Theodorou, GSMA Digital Identity

Acknowledgements:
We would like to extend our gratitude to the GSMA Policy Group, GSMA colleagues and the employees of mobile operators in 31 countries who participated in this study.

This initiative has been funded by UK aid from the UK government and is supported by the GSMA and its members.

The views expressed do not necessarily reflect the UK government's official policies.

Contents

COMMERCIALLY SUSTAINABLE ROLES FOR MOBILE OPERATORS IN DIGITAL ID ECOSYSTEMS

List of figures and case studies

Executive summary

COMMERCIALLY SUSTAINABLE ROLES FOR MOBILE OPERATORS IN DIGITAL ID ECOSYSTEMS

Customer proof-of-identity requirements for SIM registration and mobile money Know Your Customer (KYC) requirements are often regarded by mobile network operators (MNOs) as costly compliance obligations that can exclude customers who do not have the requisite identity documents (ID).

However, research by the GSMA Digital Identity programme has revealed that when a digital ID ecosystem has been built properly and supported by the public and private sector, ID verification during customer on-boarding can provide commercial benefits and opportunities for MNOs. It may also help governments meet public policy objectives and enable access to life-enhancing services for previously underserved customers.

In over 157 countries, governments require MNOs to verify, or at least capture, the identity credentials of their customers during prepaid SIM registration and mobile money KYC processes. The main reasons governments cite for introducing such regulations are preventing anti-money laundering (AML), combating the financing of terrorism (CFT) and deterring criminal activities involving the use of mobile communications.

The operating (OPEX) and capital expenditure (CAPEX) required to comply with these regulations (deploying and maintaining the relevant processes) is significant, and often borne exclusively by MNOs. MNOs must also regularly deactivate the SIM cards of existing customers who fail to register by the imposed deadline. Furthermore, it is estimated that one billion people globally do not have any form of officially recognised identification, such as a birth certificate or national ID.[1] These people live predominantly in low- and middle-income countries (LMICs) and are most at risk of being digitally, financially and socially excluded due to being unable to comply with proof-of-identity requirements. Most of the MNOs that participated in this research study confirmed they are often unable to on-board customers for this reason.

Given the current momentum for digital transformation in LMICs, which has been accelerated by COVID-19, governments are increasingly requiring MNOs to verify (rather than just capture) the identity credentials of their customers during SIM registration and mobile money KYC processes. Having a robust digital identity ecosystem in place is a core component of this. While ID verification could empower MNOs to offer value-added and personalised services to their identified and underserved customers, no substantive research has been conducted to date on the costs, benefits and opportunities of ID verification compliance for MNOs.

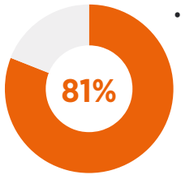
The GSMA Digital Identity team therefore embarked on research with MNOs in 31 countries, predominantly LMICs, to provide the mobile industry with benchmark costs and evidence of the benefits to inform their response to new SIM registration and electronic KYC (e-KYC) requirements. The research also identified opportunities, beyond regulatory compliance, to offer commercially sustainable and socially impactful services. For example, mobile-enabled ID verification and KYC services for insurance, education or healthcare that include traditionally underserved groups.

1 The World Bank. (n.d.). "**ID4D Data: Global Identification Challenge by the Numbers**".

Findings from the research revealed:

ECOSYSTEM

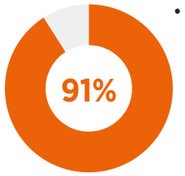
Digital transformation is accelerating and appears to be turning SIM registration and mobile money KYC rules from a mere compliance obligation into an opportunity for MNOs.



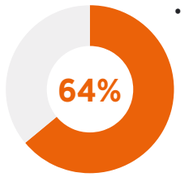
- **81 per cent** of MNOs see the positive opportunities of customer ID verification processes, primarily the provision of new products and services;
- Just over a third (**38 per cent**) of MNOs surveyed reported that they already, or plan to, harmonise and/or digitise their ID verification capabilities for SIM registration and mobile money KYC; and
- The majority (**81 per cent**) of MNOs are willing to advocate to governments for harmonisation of their SIM and mobile money customer identity verification processes, which could lower the barrier to access for mobile services and improve customer journeys.

BENEFITS

While regulatory compliance was the core benefit identified by all MNOs that invest in robust KYC processes, many also consider it a sound commercial decision.



- **91 per cent** of MNOs with digital SIM registration and mobile money KYC processes feel that knowing their customers better allows them to offer more personalised services that could drive financial inclusion among underserved communities; and



- **64 per cent** of MNOs with digital SIM registration and mobile money KYC processes consider the development of new and commercially sustainable services a core benefit. Several MNOs report that they have already increased revenue through such services.

OPPORTUNITIES

Offering ID-linked mobile financial services (aside from mobile money) currently appears to be the greatest revenue-earning opportunity for MNOs keen to invest in digital ID verification.

- MNOs that can verify customers' digital ID against a database/smartcard (e.g. government maintained) are, on average, **two times more likely** to launch ID-linked mobile services capable of empowering more underserved customers;

- The most-launched services by MNOs appear to be beneficiary verification for social cash transfers (**32 per cent of MNOs**) and ID verification or KYC for financial services (e.g. loans) (**>31 per cent of MNOs**);
- The most appealing future opportunities for MNOs are insurance (**47 per cent**) and beneficiary verification (**49 per cent**), as well as facilitating national ID enrolment, supporting health/vaccinations and providing verification for different industry verticals; and
- **Around half** of MNOs are not satisfied with their existing on-boarding processes and are interested in investing in and developing their capabilities to verify IDs against a database/ smartcard, which could then be used to develop promising ID-linked mobile services (e.g. in beneficiary verification, insurance and health contexts).

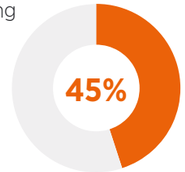
MNOs have a strong appetite for partnerships with innovators in the digital identity space.

- The majority (**61 per cent**) of MNOs are willing to work with third-party digital ID innovators in the future, while up to **31 per cent** have worked with these parties already;
- MNOs that have worked with innovators have collectively launched **at least eight** different ID-linked mobile services; and
- MNOs with digitised ID verification processes are **more likely** to have worked with innovators.

COSTS

The upfront costs for MNOs (CAPEX) to invest in SIM registration and mobile money KYC processes tend to increase with more robust digital implementations. For example:

- Implementations involving digital ID verification processes cost over **six times more** than non-digital ones, requiring an average investment of $1 million to $3 million, and in some cases up to $25 million. MNOs that have invested in verifying IDs against a database/smartcard (e.g. government maintained) incur the most costs;
- Of the MNOs capable of verifying IDs against a government database, **45 per cent** pay ID verification fees for each query (averaging 28 cents), although some report that they pay a monthly fee (averaging $7,500 a month) instead;



- Most MNOs (**55 per cent**), however, do not pay fees to query government ID databases as ID verification is considered to be in the public's interest;
- Interestingly, despite the associated costs, **52 per cent** of all MNOs in this study reported that their SIM registration/KYC ID verification processes could be more robust if they were able to verify IDs against a government-maintained database/smartcard; and
- Enabling policy environments are key. MNOs that are confident they can reap the benefits of digital ID verification are investing, on average, **250 per cent** more in their SIM registration/KYC on-boarding processes.

THREATS

While MNOs with more digitally sophisticated ID verification processes perceive fewer threats overall, most identify some threats with their SIM registration and mobile money KYC processes:

- **73 per cent** of MNOs perceive the possibility of non-compliance with the regulations as a threat;
- **80 per cent** of MNOs perceive the potential liability for SIM or wallet-related theft, fraud and criminal activity as a threat; and
- **57 per cent** of MNOs are often unable to on-board customers because they **lack the requisite identity credentials.**

COVID-19

As a result of the restrictions imposed during the COVID-19 pandemic, various MNOs were permitted to relax their ID requirements for SIM registration and mobile money KYC on-boarding. This has not only demonstrated their ability to facilitate access to mobile services for underserved communities and customers who are social distancing,[2] but also accelerated the digital transformation plans of some MNOs.

Among MNOs that relaxed their ID requirements:

- Up to **88 per cent** used remote on-boarding (e.g. remotely on-boarding oneself via one's mobile phone);
- Up to **63 per cent** relaxed ID registration terms (e.g. accepted a wider range of IDs);
- Up to **29 per cent** used tiered registration requirements (a risk-based approach); and
- Up to **29 per cent** permitted agents to visit customers' homes (e.g. to complete enrolment processes).

Most of the relaxations were mandated by government policies and are temporary in nature, although some MNOs and/or governments have put voluntary and/or longer-term measures in place.

Based on the findings of the research, the GSMA offers several recommendations for MNOs and government policymakers, including to:

- **Facilitate a conducive policy environment for the development of an inclusive, trusted and participatory digital identity ecosystem;**
- **Incentivise the exploration of public-private partnerships (PPPs) to make proof-of-identity processes more robust while leveraging MNOs' capabilities and nationwide reach; and**
- **Build on the momentum for digital transformation to support the digital, financial and social inclusion of underserved populations.**

2 Lowe, C. et al. (2021). **Digital identity: accelerating financial inclusion during a crisis**. GSMA.

1 Introduction

COMMERCIALLY SUSTAINABLE ROLES FOR MOBILE OPERATORS IN DIGITAL ID ECOSYSTEMS

It is estimated that around one billion people do not have any form of officially recognised identification, such as a national identity card or birth certificate.[3] Eighty-two per cent of these people live in low- and middle-income countries (LMICs) in South Asia and Sub-Saharan Africa,[4] where it is often the poorest (around 40 per cent) who are most in need of identity documents (ID), but have the least access to them.[5]

Even among those who have an ID, many lack evidence of a digital identity.[6] Where national identity systems have been rolled out, implementation is often beset by high or ongoing costs, the loss of paper-based records, geographic constraints, complex administration and requirements and lack of demand.[7]

The ability to officially identify oneself is necessary to participate in society. Not having an ID can lead to social and economic exclusion, threatening the employment and earning potential of billions of citizens and having a negative impact on national economies.[8,9] The United Nations Sustainable Development Goal (SDG) 16.9 aims to provide a legal identity for all by 2030.[10]

A high level of identity assurance is increasingly required to access essential services in the digital economy, from mobile-enabled insurance and credit to agricultural assistance, mobile money, education, healthcare and voting. Presenting an acceptable form of ID is legally required in at least 157 countries to register a prepaid SIM card.[11] Most mobile subscriptions in LMICs, especially in Africa, are prepaid.[12] SIM registration is carried out by mobile network operators (MNOs) that may verify officially recognised IDs or national identity cards, sometimes alongside biometrically captured fingerprints. Consequently, a lack of identification can exclude people from accessing mobile services in their own name.[13]

Access to mobile phones and the internet has driven financial inclusion, with 69 per cent of adults globally using formal financial services like mobile money. However, documentation and identification requirements for KYC processes can be a significant barrier to access and have left 1.7 billion people financially excluded.[14,15,16]

Digital inclusion, such as mobile and internet access, is considered a key enabler of 13 of the 17 SDGs.[17] Governments have a role to play in providing citizens with an official national ID — a foundational ID that an individual can use for general identification and public administration purposes. A functional digital ID, on the other hand, can be created from various attributes and may be used for a specific purpose or function.

3 The World Bank. (n.d.). "ID4D Data: Global Identification Challenge by the Numbers".
4 Ibid.
5 World Bank Group. (2017). Identification for Development: Africa Business Plan.
6 McKinsey Global Institute. (2019). Digital Identification: A Key to Inclusive Growth.
7 Benson, C. et al. (2017). Digital Financial Services: Ecosystem.
8 Gelb, A. and Clark, J. (2013). Identification for Development: The Biometrics Revolution. CGD Working Paper. 315. Center For Global Development.
9 Mastercard. (2019). Digital Identity: Restoring Trust in a Digital World.
10 United Nations Sustainable Development Goal (SDG) 16: https://sdgs.un.org/goals/goal16
11 Theodorou, Y. and Yongo, E. (2020). Access to mobile services and proof-of-identity 2020: The undisputed linkages. GSMA.
12 Theodorou, Y. and Yongo, E. (2018). Access to mobile services and proof-of-identity: Global policy trends, dependencies, and risks. GSMA.
13 Ibid.
14 Ibid.
15 FATF. (2020). International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations.
16 The World Bank. (2017). Global financial inclusion and consumer protection survey.
17 United Nations. (2018). Igniting SDG progress through digital financial inclusion.

Where governments have provided national IDs, and increasingly if they are inclusive and digitally enabled, there can be opportunities for MNOs to upgrade and digitise their SIM registration and mobile money KYC ID verification processes. This can provide previously underserved customers and communities with faster, more efficient, robust and trusted solutions that are less prone to fraud.[18]

Several countries in Africa have encountered challenges with national IDs. While some governments have invested in digital ID ecosystems, poor national ICT infrastructure has meant registration points are still unconnected. Other countries, including those with national ID smartcards, lacked the ability to verify individuals digitally or against civil registries.[19] However, with an almost unparalleled ability to reach the majority of a country's population, businesses and across borders, MNOs are well placed to facilitate digital identity. Whether by supporting national ID enrolment[20] or leveraging customer attributes from their SIM registration or mobile money KYC processes, MNOs can support the creation of functional digital identities that can be used to access mobile and e-government services.

The potential opportunities created by digital ID, including digital/financial inclusion and commercial benefits, have rapidly expanded due to better mobile and internet access and increasingly sophisticated verification and authentication technologies (cards, biometrics and virtual).[21] However, most MNOs are required by regulation from telecommunication authorities (for SIM registration) and central banks (for mobile money KYC) to verify the identity of their customers to prevent the use of mobile for acts of terrorism, money laundering and all other forms of criminal activity. Compliance with these requirements puts greater demands on MNOs, from spending more time on-boarding customers to higher CAPEX and OPEX and ID verification fees. Compliance can also create an inefficient and unreliable on-boarding process and customer journey, which may have a negative impact on customer trust and, in turn, the MNO.[22]

Well-planned and implemented digital on-boarding and ID verification can help MNOs meet these increased demands by making these processes more robust and creating new ways to leverage these assets. Digitisation can also improve access to, and increase demand for, mobile and mobile-enabled digital services by establishing, strengthening and simplifying digital identity verification processes for customers. It can also provide a plethora of new commercially sustainable and socially impactful ID-linked services.[23,24]

While the requirement to verify customer IDs brings both costs and potential benefits to MNOs, there has been little research to date that has assessed and benchmarked the costs, benefits and opportunities for MNOs to invest in ID verification capabilities beyond regulatory compliance. The GSMA Digital Identity team therefore conducted research to enable the mobile industry to better assess the costs and benefits, respond to new SIM registration and e-KYC requirements and identify opportunities to offer commercially sustainable and socially impactful value-added services, such as ID verification and KYC services for insurance, education and healthcare.

18 Theodorou, Y. and Yongo, E. (2018). Access to mobile services and proof-of-identity: Global policy trends, dependencies, and risks. GSMA.
19 Clark, J. (2017). The state of identification systems in Africa: A synthesis of country assessments. The World Bank.
20 For example, in Nigeria in 2020/21: https://nimc.gov.ng/docs/Approved_Data_Capturing_Agents.pdf
21 The World Bank (2017). Technology Landscape for Digital Identification, Identification for Development.
22 Wilson, M. and Waddington, R. (2019). Understanding capture and validate KYC processes: global experiences, challenges and learnings. GSMA.
23 Ibid.
24 Theodorou, Y. and Yongo, E. (2020). Access to mobile services and proof of identity 2020: the undisputed linkages. GSMA.

COMMERCIALLY SUSTAINABLE ROLES FOR MOBILE OPERATORS IN DIGITAL ID ECOSYSTEMS

1.1 Scope

This study investigates the ID verification landscape in 31 countries, predominantly LMICs. It focuses on ID verification for SIM registration and mobile money KYC processes, and considers the ecosystems, benefits, opportunities, costs and threats of ID verification for MNOs. It also reviews how these processes were modified to respond to the COVID-19 pandemic.

This study does not claim to be exhaustive or representative of MNOs or the countries or regions where the research was conducted. Rather, this study is a contribution to the digital identity landscape and the mobile industry's position within it.

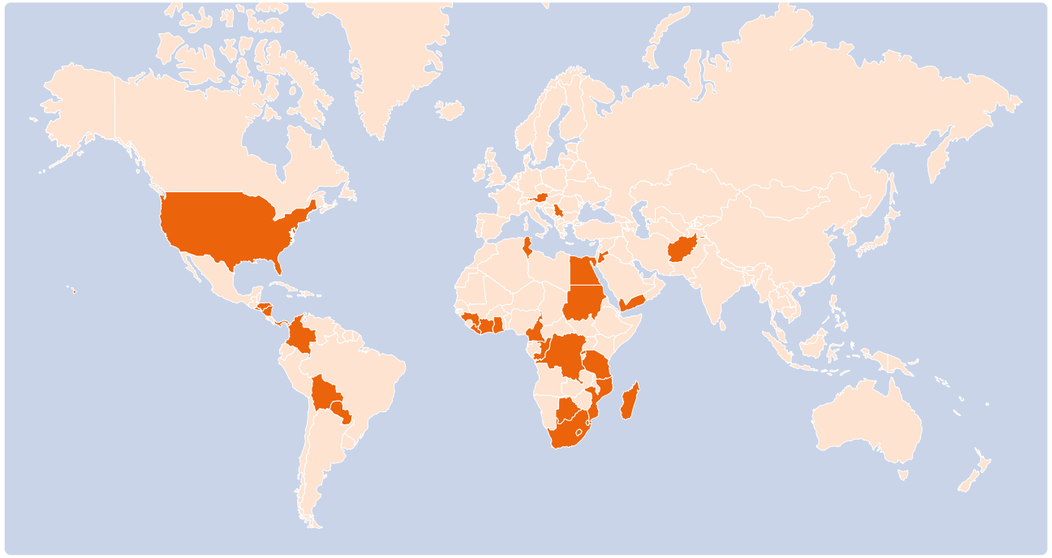
Desk research and a literature review were conducted to assess the prevalence and variety of ID verification methods used for SIM registration and mobile money KYC mandates, particularly in LMICs. The results were used to identify a mix of countries where MNOs employ different methods of physical and digital ID verification to comply with local SIM registration and KYC regulatory requirements.

An in-depth survey was completed by participants from MNO policy, legal and regulatory teams, in addition to other relevant business units at MNOs in every country. Where required, the Digital Identity team followed up with respondents to explore topics in more detail or to clarify answers. The research findings presented in this report are anonymous and aggregated to ensure confidentiality, and most detail at the country or corporate level has been avoided. Monetary references have also been aggregated and presented as ranges.

Various MNOs in the following countries participated in the research: Afghanistan, Austria, Bolivia, Botswana, Cameroon, Colombia, Congo, Côte d'Ivoire, Democratic Republic of Congo (DRC), Egypt, El Salvador, Eswatini, Ghana, Guinea, Honduras, Jordan, Lesotho, Liberia, Madagascar, Mozambique, Nicaragua, Panama, Paraguay, Rwanda, Serbia, South Africa, Sudan, Tanzania, Tunisia, United States and Yemen (Figure 1).

Figure 1

The GSMA conducted primary research with MNOs in 31 countries



2 ECOSYSTEM

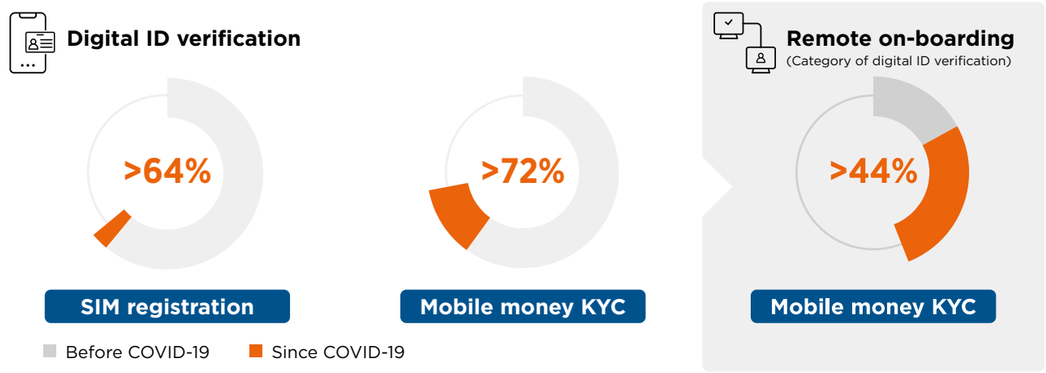
Digital transformation is turning SIM registration from a burden into an opportunity

The benefits of robust SIM registration and ID verification against a database/smartcard (e.g. government maintained) include, but are not limited to, a better customer experience, simpler customer journey, greater privacy and data security, access to a variety of mobile-enabled services, cost savings, simplified processes, richer data and the ability to know customers better.[25] MNOs in this study use a variety of ID verification methods for SIM registration and mobile money KYC. While these methods are not necessarily representative of all MNOs or the countries or regions where they operate, they provide a comparison and industry benchmark.

The majority of MNOs in this study employed KYC processes for mobile money in addition to SIM registration (see Figure 3). Most MNOs store customer ID credentials as part of their on-boarding process while a few share ID credentials with their government. However, a growing number of MNOs have implemented more robust ID verification against a government-maintained database/smartcard, a sign that MNOs and governments are willing to collaborate and advance their digital transformation agendas. This is more prevalent for mobile money KYC since ID requirements for basic accounts and tiered KYC are often (but not always) more stringent, and a greater barrier to underserved individuals, than requirements for SIM registration due to anti-money laundering (AML) and combating the financing of terrorism (CFT) regulations, among others.

Figure 2

Digital transformation has advanced the ID verification capabilities of MNOs while COVID-19 measures have accelerated them



Base: All respondents; Question: What type of mandatory SIM registration do you operate in your country? Question: Do you offer mobile money (KYC) in your country? Question: Explain how ID verification takes place during mandatory SIM registration, and how is on-boarding to mobile money (KYC) different? Question: In response to COVID-19, what are the relaxed measures?

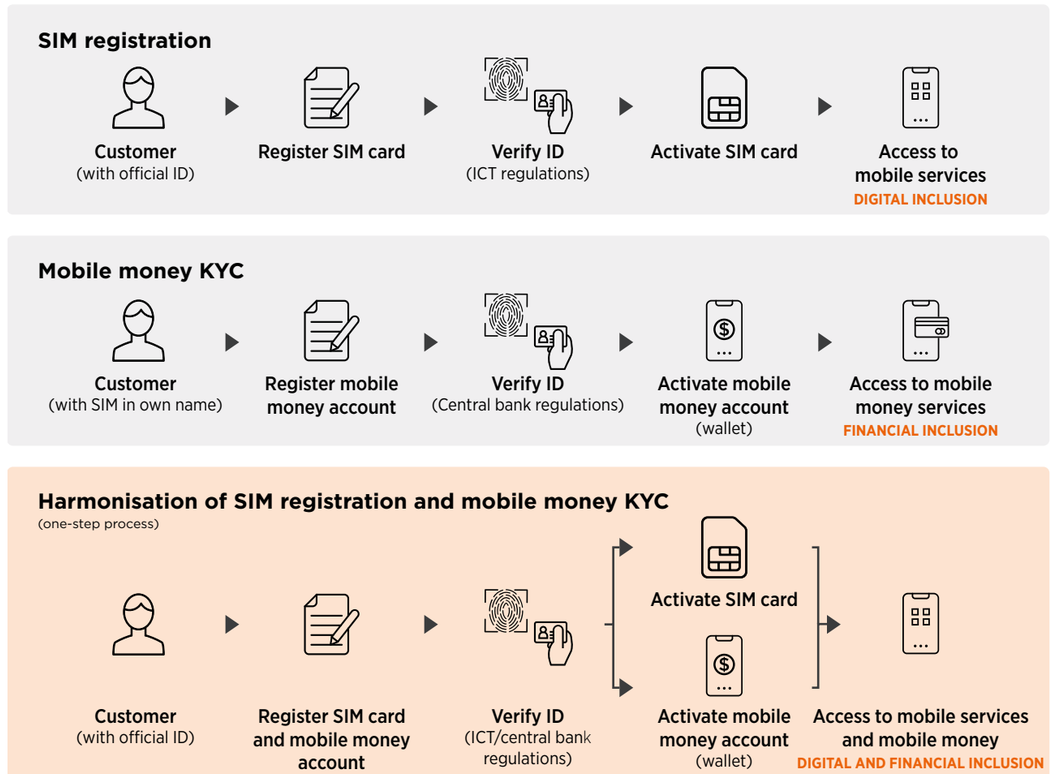
25 Wilson, M. and Waddington, R. (2019). Understanding capture and validate KYC processes: global experiences, challenges and learnings. GSMA.

The level of digitisation of ID verification processes varies among MNOs in this study. MNOs either have digital ID verification capabilities (e.g. digital ID cards, biometrics, ID verification against a database/smartcard, remote on-boarding) or physical, non-digital capabilities (see Figures 4 and 5). MNOs with digital ID verification capabilities claimed that around a quarter of their customers have not been verified against a digital ID. This highlights the potential for on-boarding barriers, such as having no digital ID, relying on a family member or friend to register on one's behalf or not seeing the value of having one's SIM card registered against a verifiable ID in one's own name.

Sixty-one per cent of MNOs in this study are able to verify customer IDs digitally for SIM registration, and this rose to 64 per cent during the COVID-19 pandemic as digital transformation picked up speed (Figure 2). This has been more pronounced for mobile money KYC. The percentage of MNOs verifying customer IDs digitally for mobile money KYC rose from 60 to 72 per cent. Even more outstanding is that the number of MNOs capable of supporting remote ID verification (whether temporarily or permanently) rose from 16 to 44 per cent during the COVID-19 pandemic due to efforts to digitally and financially include citizens and customers. This signifies a willingness and flexibility on the part of MNOs and governments to ensure citizens could still access mobile services despite restrictions on movement and social distancing.

Figure 3

SIM registration and mobile money KYC on-boarding methods

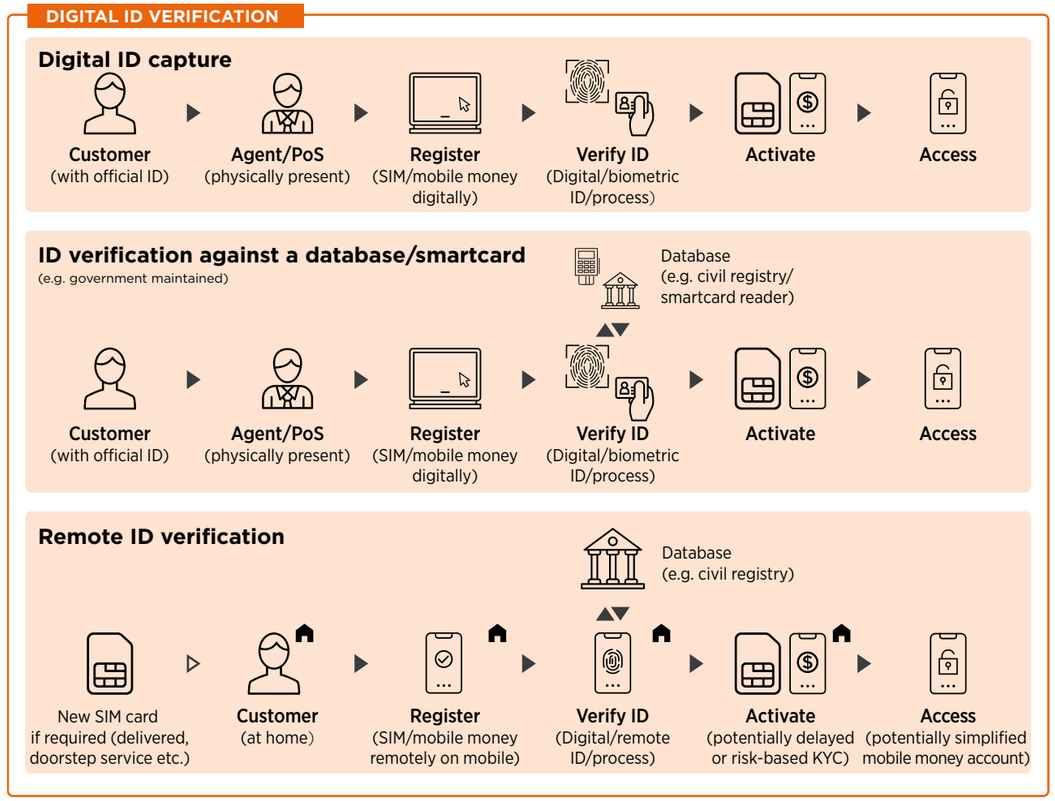


Note: Processes have been simplified for comparison

SIM registration and KYC on-boarding methods vary from physical to digital and biometric.

Figure 4

ID verification methods for SIM registration and mobile money KYC

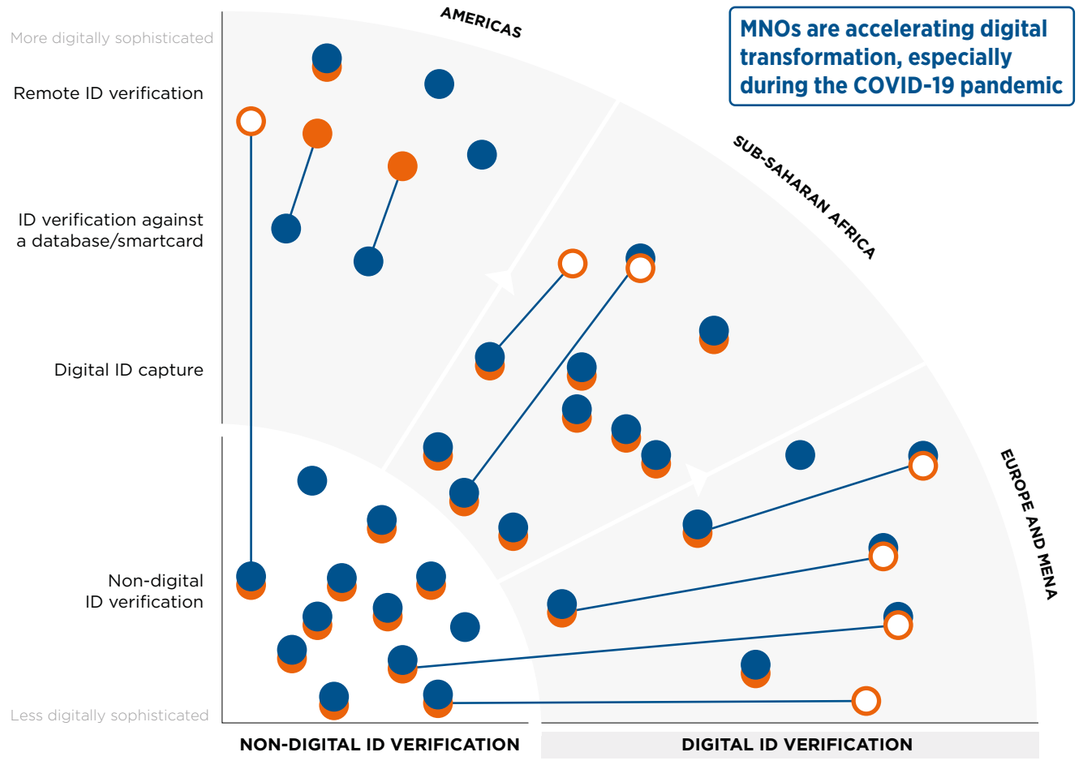


Note: Processes have been simplified for comparison

Remote on-boarding or verification performed on one's mobile phone is a more nascent method of ID verification. A recent example of remote verification for SIM registration is Vodacom South Africa's self-RICA and TOBI applications, which allow customers to on-board themselves at home.[26]

Figure 5

The digital sophistication of MNOs' ID verification capabilities for SIM registration and mobile money KYC, and digital acceleration during the COVID-19 pandemic



Notes: Bubbles represent the countries where MNOs in this study are located. ID verification capabilities may vary between MNOs in each country, not all MNOs in each country have been analysed. Some capabilities may have changed. **SIM registration –** the on-boarding process required to obtain a SIM card in one's own name involves different methods of official ID verification, such as MNOs capturing and keeping a record of their customers' information, proactively capturing and sharing customers' information with a government/regulator and verifying customers' ID credentials against a database/smartcard (e.g. government-maintained or otherwise, mandated or otherwise). These may be digital or not. **Mobile money KYC –** the on-boarding process required to obtain a mobile money account/wallet. **COVID-19 response –** bubbles represent the countries where MNOs reported they have enabled new digital on-boarding methods to ensure social, financial and digital inclusion during the COVID-19 pandemic. **Remote ID verification –** this may include, for example, the ability to on-board oneself via one's mobile phone. **ID verification against a database/smartcard –** verification of ID against a database or smartcard (e.g. government/civil). **Digital ID capture –** capturing and storing/sharing digital ID credentials rather than verifying against a database/smartcard (e.g. a civil database). **Digital ID verification –** all digital forms of ID verification. **Non-digital ID verification –** verification is often physical, in person and may be paper-based and involve travel to agents or points of sale (PoS).
Source: GSMA primary research with MNOs in 31 countries, GSMA data and analysis

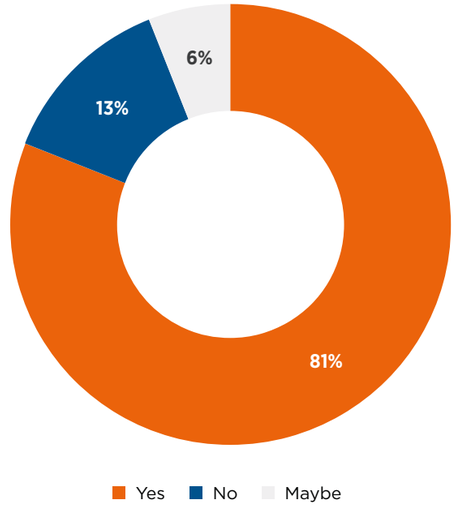
26 https://now.vodacom.co.za/article/a-simplified-self-rica-process-from-vodacom

Governments and MNOs in some countries have accelerated their digital transformation efforts in response to COVID-19. Digital methods of on-boarding customers to mobile, such as remote self-registration, have supported digital and financial inclusion during the pandemic.

81 per cent of MNOs consider SIM registration and KYC mandates a positive opportunity. When asked to explain why, the most frequent answer was "to provide new products and services".

Figure 6

81 per cent of MNOs consider SIM registration and mobile money KYC mandates a positive opportunity



Top 10 reasons why MNOs consider the mandates a positive opportunity

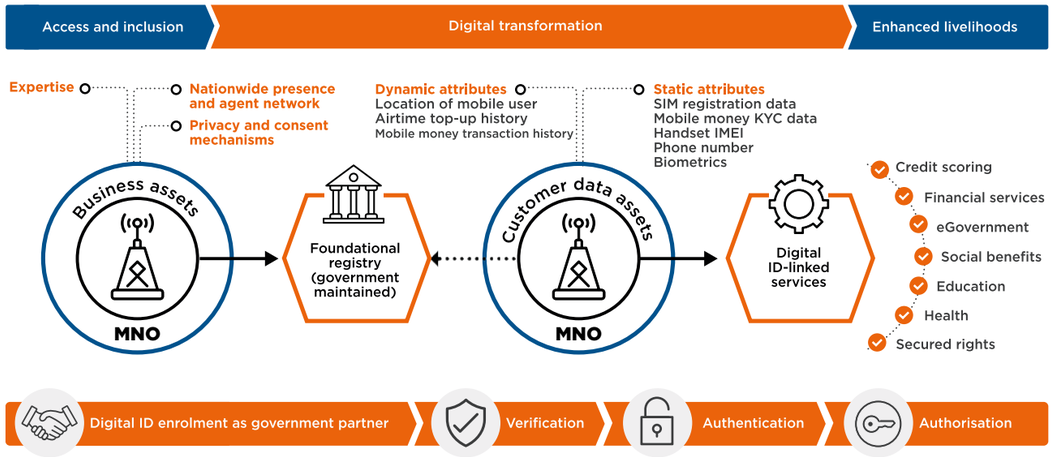
1. Provide new and appropriate products and services
2. Prevention of fraud, AML, cybercrime and other crime
3. Understand customers and spending patterns better
4. Improve national security/supply information
5. Improved customer database
6. Support government
7. Improve customer access to mobile-enabled services
8. Support customer mobility
9. Security of SIM user and family
10. Simplification of on-boarding process

Base: All respondents. Question: Looking to the future, do you now consider SIM registration and KYC mandates a positive opportunity rather than a burden? Please explain.

Regardless of digital sophistication, on-boarding modalities and costs, most MNOs in this study (81 per cent) consider SIM registration and mobile money KYC mandates as positive strategic opportunities (Figure 6). While there is a significant upfront investment in setting up these processes and on-going operational costs to adhere to these mandates, MNOs cited various positive opportunities and benefits for their organisations, governments and citizens alike.

Figure 7

The costs, benefits and opportunities of MNO ID verification processes for SIM registration, mobile money KYC and ID-linked mobile services

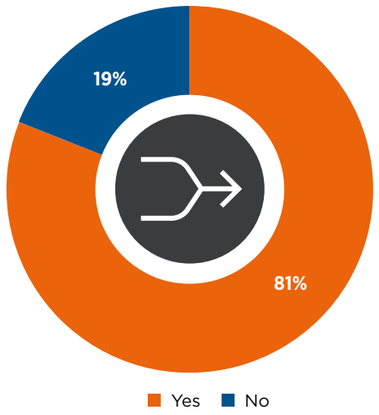


MNO respondents noted that in order to maximise the potential benefits of linking customers' mobile subscriptions with proof of identity, they would need to develop robust on-boarding processes with ID verification capabilities, and customers would need to possess an appropriate official ID (see Figure 7).

If MNOs can make their SIM registration and mobile money KYC on-boarding processes sufficiently robust, they believe they could advance digital and financial inclusion for citizens, achieve commercial sustainability and support their government (see Figure 8).

Figure 8

81 per cent of MNOs are willing to advocate for the harmonisation of SIM registration and mobile money KYC compliance processes



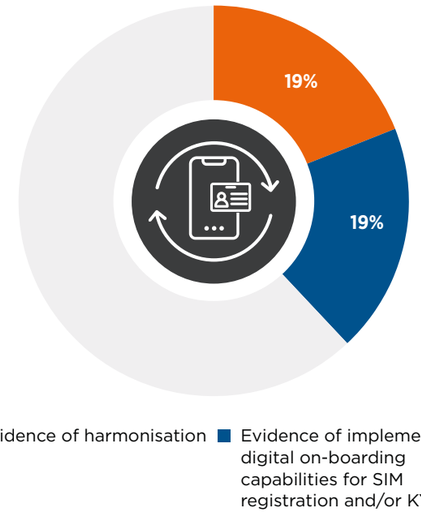
Harmonising SIM registration and mobile money KYC ID verification processes could lower barriers for the most underserved to access mobile services in their own name.

Base: All respondents. Question: Would you be willing to advocate to harmonise SIM-registration with KYC to offer customers better mobile-linked services, for example, requiring only one visit to register?

Harmonising SIM registration and mobile money KYC requirements can simplify on-boarding for all parties and, if implemented well, can lower the investment and operational costs for MNOs to fulfil the mandates. A simpler, quicker on-boarding experience may also promote customer loyalty. Robust ID verification, coupled with MNOs' data protection and privacy practices, has the potential to build customer trust and provides a platform for MNOs to offer ID-linked mobile services. With the potential to lower barriers to customer on-boarding, harmonisation provides an opportunity for MNOs to drive both social inclusion and commercial sustainability.

Figure 9

38 per cent of MNOs show evidence of harmonisation and implementation of digital on-boarding



Digital ID ecosystems are driving harmonisation of SIM registration and KYC regulatory compliance processes.

Base: All respondents

Various MNOs in this study have made progress in harmonising SIM registration and mobile money KYC on-boarding processes (see Figure 9). For example, enabling a one-step-process in which a customer only needs to provide their official identification credentials once to access both an active SIM/mobile phone and a mobile money account. Several other MNOs in this study have either already implemented, or are planning to implement, more digitally sophisticated SIM registration and mobile money KYC processes, and are incorporating digital IDs, biometric capabilities and/or ID verification against a database/smartcard (e.g. government maintained). However, these implementations can be complex and difficult to complete.

Despite MNO investment in digital ID verification capabilities, the onus remains on governments to ensure the entire population has access to an official digital ID credential. This would allow them to ensure customer identification processes use digital technologies and support more seamless harmonisation of SIM registration and mobile money KYC requirements.[27] In this study sample, around a quarter of the customer base of MNOs with digital ID verification capabilities use non-digital forms of identification.

Adoption of digital forms of ID is far from complete. Of the countries in this study that allow the use of digital IDs for SIM registration and mobile money KYC, over 25 per cent of MNO customers still use non-digital forms of ID.

Summary

Most MNOs in this study recognise the positive benefits of SIM registration and mobile money KYC mandates, from regulatory compliance and combating criminal activity to empowering customers, protecting their data and privacy and the commercial opportunities of ID-linked services. Another major benefit is greater digital and financial inclusion, especially for the most underserved.

MNOs appear to be implementing more digitised ID verification processes (such as ID verification against a database or smartcard), and most are willing to advocate for harmonising SIM registration and mobile money KYC. MNOs have accelerated digital transformation during COVID-19 (e.g. with remote on-boarding) due to the need to include customers and citizens digitally and financially amid restrictions on movement and social contact. **The acceleration of digital transformation seems to be turning SIM registration and mobile money KYC rules from a compliance obligation into opportunities for MNOs.** There is also an opportunity for policymakers to work more closely with MNOs to develop conducive ID verification ecosystems that meet the requirements of governments, MNOs and citizens.

27 Theodorou, Y. and Yongo, E. (2020). Access to mobile services and proof of identity 2020: the undisputed linkages. GSMA.

COMMERCIALLY SUSTAINABLE ROLES FOR MOBILE OPERATORS IN DIGITAL ID ECOSYSTEMS

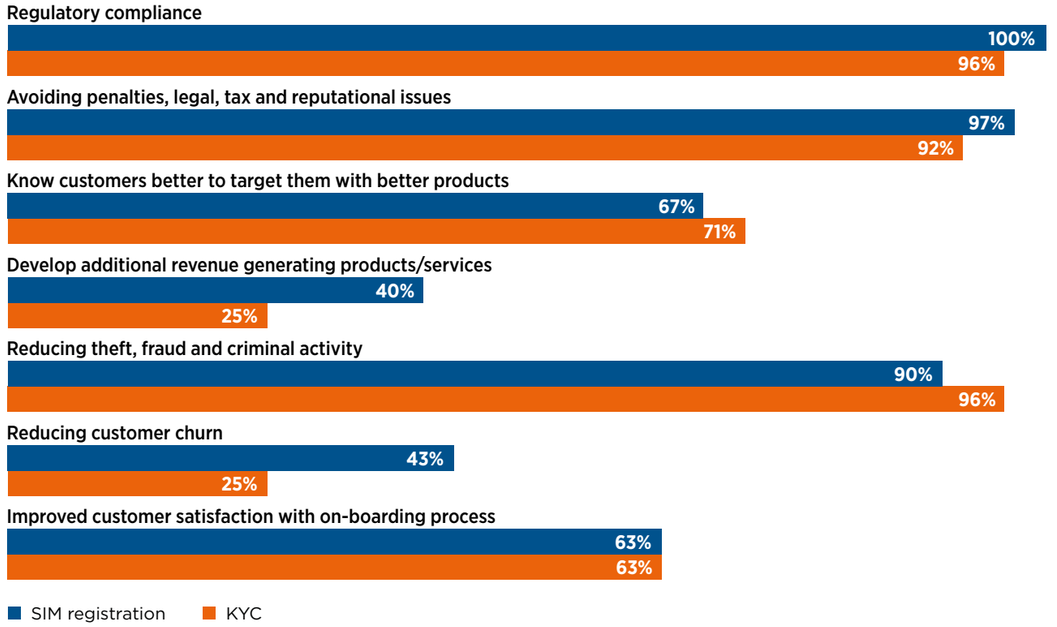
3

BENEFITS

Regulatory compliance is at the top of the list and many MNOs consider it a commercial opportunity

Figure 10

The benefits of investing in SIM registration and mobile money KYC processes



Base: All respondents. Question: What are the main benefits of your investment in SIM registration and KYC?

Regulatory compliance, avoiding penalties and reducing criminal activity are the main benefits

All MNOs cited regulatory compliance; avoiding penalties, legal, tax and reputational issues; and reducing theft, fraud and criminal activity as the main benefits of investing in their SIM registration and mobile money KYC processes (Figure 10).

Compliance risk remains a primary concern. MNOs might consider digital identification and verification services a risk to their customers' personal data security. However, MNOs that verify smartcard IDs or biometric impressions against a database often do not keep that data. Instead, they typically query the database and receive either a 'yes' or 'no' response to confirm an ID is genuine.

Digital identification and verification services do not, therefore, elevate compliance risk. For example, in a health context, an MNO would be a 'technology enabler' to help a customer access their patient/health record without having any access to, or responsibility for, the customer's data. Furthermore, MNOs could offer ID Verification as a Service (VaaS) for third parties, such as disbursing social benefit payments to intended beneficiaries by confirming that a beneficiary's KYC details match those of the benefit provider.

Customer-focused commercial opportunities are another main benefit

Forty per cent of MNOs see developing additional revenue-generating products and services as one of the main benefits of investing in SIM registration processes. Half of these MNOs either already have developed, or are developing, digital ID-linked and/or ID verification services. Further evidence of MNO interest in commercial services and social inclusion is that 71 per cent of MNOs (67 per cent for SIM registration) would like to know their customers better and deliver better products by leveraging KYC.

Some MNOs mentioned the commercial possibilities of ID verification and that SIM registration and KYC are not being used to their full potential.

> [We] on-boarded several million customers per year [to SIM cards] since [having the] ability to [properly] identify customers during SIM registration.

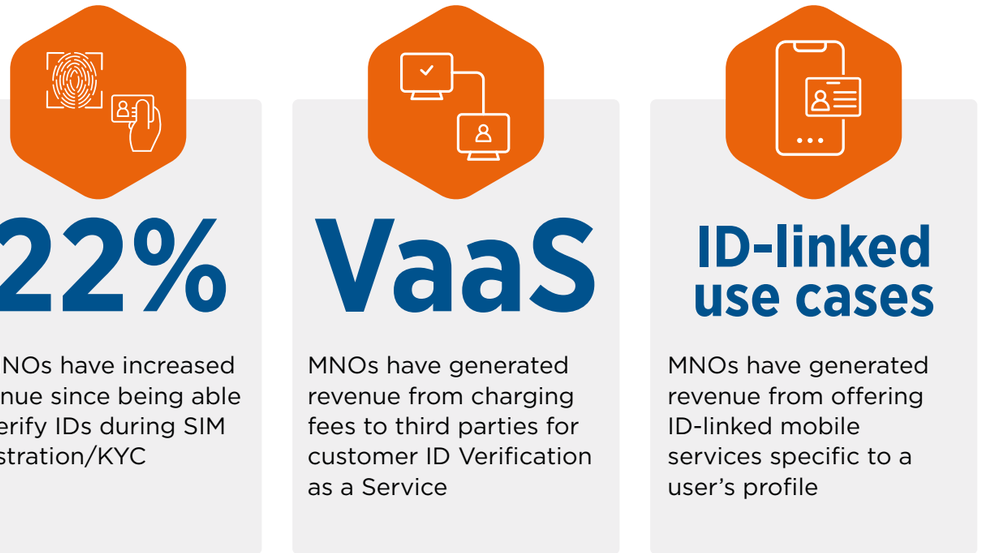
> MNOs [are] not leveraging SIM registration/KYC to its maximum benefit to deliver sustainable business models.

In some countries, data protection and privacy laws prohibit commercial activity.

> Commercial activity by MNOs (using customer on-boarding data) is not allowed; only companies such as banks and financial service providers (e.g. mobile money providers) have permission [to pursue commercial opportunities].

Figure 11

MNOs have benefited commercially from leveraging SIM registration and KYC



Base: MNOs reporting revenue changes. Question: How has your revenue changed since introducing SIM registration and KYC? Notes: VaaS (Verification as a Service) – for example, when MNOs use SIM registration/mobile money KYC processes to verify the identity of third-party customers. ID-linked use cases – a mobile app/service offered by an MNO that is accessed by and tailored to a customer's personal details (typically provided during SIM registration/mobile money KYC on-boarding)

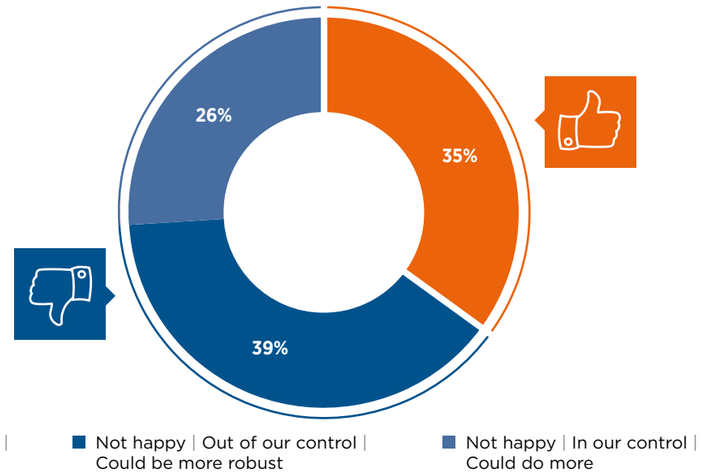
Several MNO respondents (around 20 per cent) cited revenue increases since rolling out their ID verification processes (Figure 11). Some MNOs are also benefiting fiscally from ID-linked mobile services and VaaS for third parties. Although evidence is limited, depending on respondents' willingness to share data, the potential positive commercial (and inclusion) effects of offering these services would merit further investigation by MNOs with digital ID verification processes.

Customer ID verification offers potential commercial and cost-saving opportunities

Identity VaaS is a commercial opportunity for MNOs to leverage their SIM registration and mobile money KYC assets to provide verification services to third parties – a market that is expected to grow.[28] There are also opportunities for MNOs to realise cost savings. In India, for example, it was estimated that Aadhaar, the national digital identity system, could reduce customer ID verification on-boarding costs from $23 to 15 cents for the average private sector company.[29] MNOs may be able to achieve cost savings for themselves (for SIM and KYC on-boarding) and their customers if they invest in robust, digitised ID verification against a database/smartcard (e.g. government maintained) in contexts where digital identities are widely available and used by the local population. Companies such as MNOs that require high levels of assurance for customer on-boarding may also be able to realise cost savings of up to 90 per cent, as well as a substantial reduction in registration times.[30]

Figure 12

A third of MNOs are satisfied with the robustness of their SIM registration and mobile money KYC processes



Base: All respondents. Question: How do you feel about the robustness of your SIM registration/KYC processes?

28 Maynard, N. and Morrow, S. (2020). Digital identity: technology evolution, regulatory landscape and forecasts 2020–2025. Juniper Research.

29 The World Bank. (2018). Private Sector Economic Impacts from Identification Systems.

30 McKinsey Global Institute. (2016). Digital Finance for All: Powering Inclusive Growth in Emerging Economies.

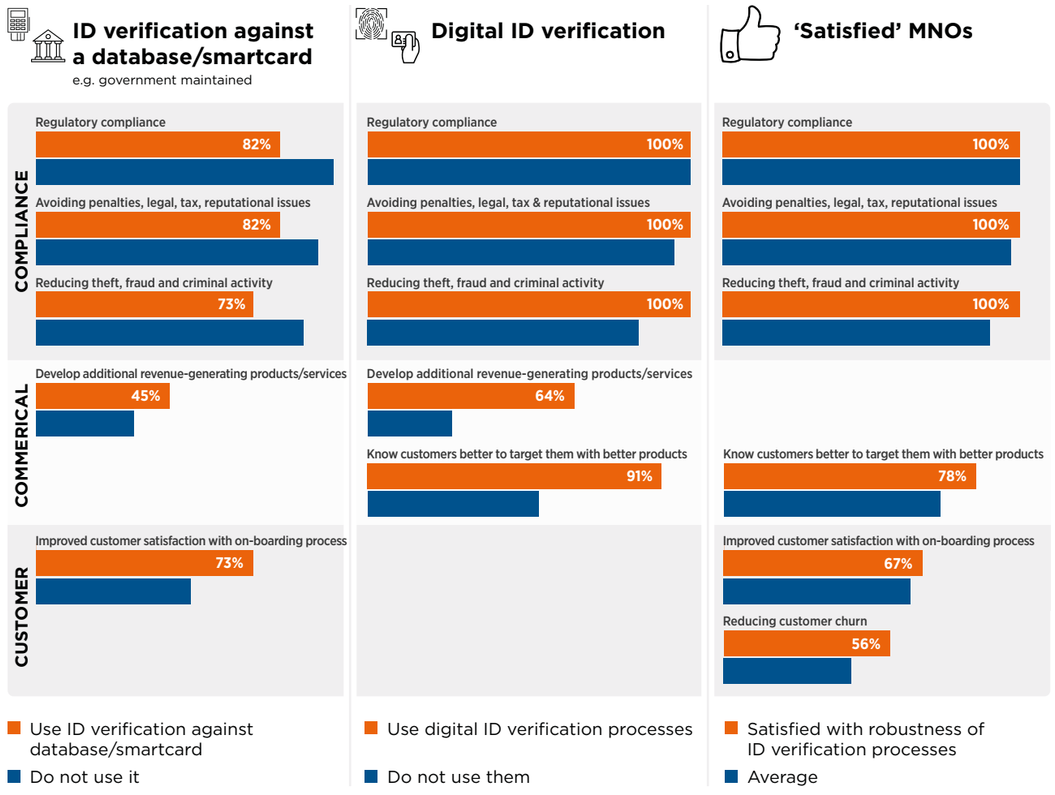
The majority (65 per cent) of MNOs in this study are not satisfied with their ID verification processes for SIM registration and mobile money KYC, but it is encouraging that 26 per cent believe it is in their control to improve (Figure 12). Thirty-nine per cent of MNOs, however, feel that the robustness of their processes is out of their control. This is where system integration issues, poor public sector collaboration, stunted roll-out of national IDs and other challenges, may be preventing MNOs from developing effective and robust SIM registration processes. **On the positive side, 35 per cent of MNOs are satisfied with the robustness of their processes.**

These MNOs tend to share certain characteristics:

- More digital ID verification capabilities;
- ID verification against a database/smartcard (but not all);
- Fewer on-boarding issues with IDs;
- More benefits from knowing customers better and launching new products;
- Robust focus on compliance, data protection/ privacy and crime;
- Invested two and a half times more, on average, in SIM registration/mobile money KYC processes;
- Lower hardware and software-related CAPEX;
- More partnerships with third parties/innovators; and
- Launched more ID-linked mobile services.

Figure 13

The main benefits for MNOs to invest in SIM registration and mobile money KYC processes



Base: All respondents. Question: What are the main benefits of your investment in SIM registration and KYC? Notes: ID verification – MNOs with the capability to verify ID against a database/smartcard (e.g. government maintained). No ID verification – MNOs without ID verification capabilities against a database/smartcard (e.g. government maintained). Digital – MNOs with all digital forms of ID verification . Non-digital – MNOs with physical, in-person and perhaps paper-based ID verification that may involve travel to agents or retailers. 'Satisfied' – MNOs that are satisfied with the robustness of their SIM registration/mobile money KYC processes

MNOs that verify IDs against a database/smartcard appear more focused on commercial opportunities and customer satisfaction than compliance, compared with MNOs that cannot verify customer IDs

MNOs that can conduct ID verification against a database/smartcard place less emphasis on regulatory compliance, avoiding penalties and reducing crime as the main benefits of their investment (Figure 13). Once a certain level of high-assurance ID verification and regulatory compliance have been achieved, it is possible that MNOs could have moved up the digital value chain and become more focused on customer satisfaction, upselling new services and reaping commercial benefits.

MNOs with digital ID verification processes appear highly focused on both compliance and commercial opportunity

All MNOs with digital ID verification capabilities view regulatory compliance, avoiding penalties and reducing crime as the main benefits of their investment. This may be due to the greater transparency of digital IDs and that several MNOs in the study do not yet have sufficiently robust processes to verify IDs against a database/smartcard. They place considerably more emphasis on knowing customers better to provide better products (91 per cent) and developing additional revenue-generating products/services (64 per cent) than those without digital ID verification capabilities. Commercial optimism may stem from having a newfound ability to leverage digital platforms and customer data, as may have been the case with MNOs that already verify IDs against databases/smartcards.

MNOs that are satisfied with their robust ID verification processes focus strongly on compliance *and* their customers

All MNOs that are satisfied with the robustness of their SIM registration and KYC processes view regulatory compliance, avoiding penalties and reducing mobile-related fraud/criminal activity as the main benefits of their investment. They are also noticeably more focused on knowing their customers better and customer satisfaction. It could be that a strong customer focus alongside robust compliance measures are generating relatively more benefit for these MNOs than others.

Summary

While regulatory compliance was the core benefit identified by all MNOs that invest in robust KYC processes, many also consider it a strong commercial decision. MNOs with digital ID verification processes focus more on compliance and commercial opportunity whereas those that verify IDs against a database/ smartcard tend to focus less on compliance (perhaps because they already have automated compliant processes) and more on customer on-boarding and new commercial activities. MNOs that are satisfied with their robust ID verification processes tend to focus strongly on compliance and their customers (suggesting that on-boarding and customer focus may be more beneficial for MNOs). There is an opportunity for policymakers to work with MNOs to facilitate robust national ID dissemination, providing a platform for developing effective and inclusive mobile-enabled ID-linked services.

COMMERCIALLY SUSTAINABLE ROLES FOR MOBILE OPERATORS IN DIGITAL ID ECOSYSTEMS

4 OPPORTUNITIES

MNOs see the potential for innovation in SIM registration and KYC, but customer trust is key

There is an opportunity for the mobile telecommunications industry to leverage their registration and KYC assets beyond compliance to benefit citizens, public institutions and their own commercial interests.

The industry has potential to offer inclusive mobile services while maintaining commercial sustainability. For example, partnerships can be built with innovative solution providers to design identity-linked digital services tailored to a customer's mobile usage. Consortiums could be assembled alongside other MNOs, ID authorities and government bodies and, by sharing costs or resources, they could implement ID verification systems more effectively and strengthen the security of digital services that rely on authenticating the identity of the user.

As more governments invest in national digital identity ecosystems, enabling the private sector to verify customers' ID credentials can support many functional applications,[31] and help to include previously underserved individuals with services such as health, banking and mobile money.[32] An example is M-Shwari, a mobile savings platform in Kenya that enables customers with a national ID that can be verified against a civil registry, to save higher balances and have access to credit. In Zambia, the GSMA has collaborated with the government and MNOs to launch mobile-enabled ID-linked social cash transfers.

In countries such as Sri Lanka and Haiti, those without access to a national ID may be able to access basic mobile money accounts with limited functionality when they register a SIM card in their own name.[33,34,35] This more simplified and risk-based approach has allowed many vulnerable people to access life-enhancing services.[36] In humanitarian settings where national IDs may not be accessible, such as in Somaliland, the GSMA has facilitated the piloting and use of a mobile-enabled voice ID (a functional ID) with a consortium that includes MNOs.[37] The solution requires a user to provide a voice signature (ID) by speaking into their mobile phone, and once the signature is confirmed they are able to receive disbursements via mobile money.

Digital ID verification also enables MNOs to save costs. For example, Paytm and Jio, an MNO in India, leveraged the national Aadhaar ID system to quickly on-board millions of merchants and customers with KYC processes.[38] This has reduced fraud and leakage from clean data sets and enabled robust ID verification.[39]

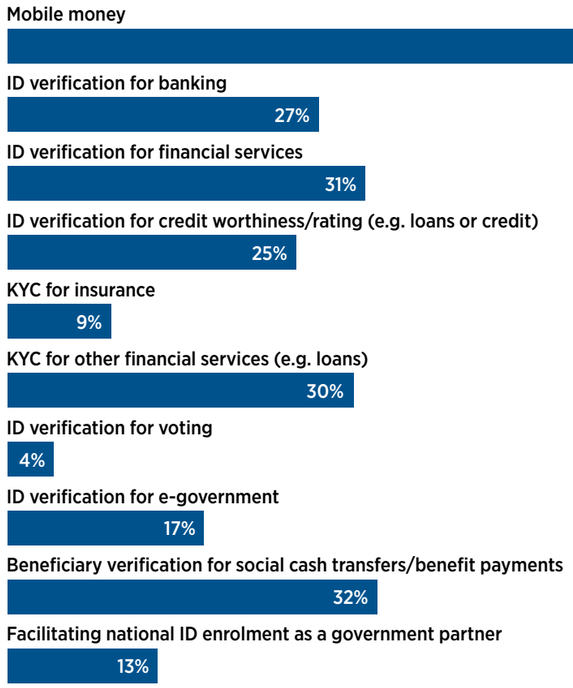
Tailoring products and services can enhance financial inclusion and customer experiences, trust and loyalty,[40] and MNOs could leverage SIM registration and mobile money KYC assets to diversify and move up the digital value chain. They could also offer digital identity-led services that should provide more value to customers, such as third-party VaaS in multiple contexts, customer on-boarding services and fraud detection. The potential for MNOs to diversify has been kick-started by rapid uptake of digital services during the COVID-19 pandemic. In general, however, there is a potential existential threat to MNOs from competing third-party digital ID-led apps.[41]

31 The World Bank. (n.d.). "ID4D Data: Global Identification Challenge by the Numbers".
32 Benson, C. et al. (2017). Digital Financial Services: Ecosystem. ITU.
33 Gelb, A. (2016). Balancing Financial Integrity with Financial Inclusion: The Risk-Based Approach to 'Know Your Customer'. Center for Global Development.
34 AFI. (2018). Digital Financial Services.
35 In many countries, identity verification is not a prerequisite for SIM registration and consumers may present several forms of functional ID, not necessarily issued by the government, such as a student ID card.
36 Kumar, K. and Radcliffe, D. (14 January 2015). Mobile Money in Pakistan: From OTC to Accounts, Part 2.
37 Mebur, J. (14 January 2021). "The Voice ID Project: Verifying recipients of mobile money supported humanitarian cash transfers in Somaliland", Mobile for Development Blog.
38 McKinsey Global Institute. (2019). Digital Identification: A Key to Inclusive Growth.
39 Ibid.
40 Lal, R. and Sachdev, I. (2015). Mobile Money Services: Design and Development for Financial Inclusion.
41 Maynard, N. and Morrow, S. (2020). Digital identity: technology evolution, regulatory landscape and forecasts 2020–2025. Juniper Research.

4.1 Current digital ID use cases: a commercial and social impact opportunity

Figure 14

MNOs are leveraging SIM registration and mobile money KYC assets to offer various digital ID-linked services

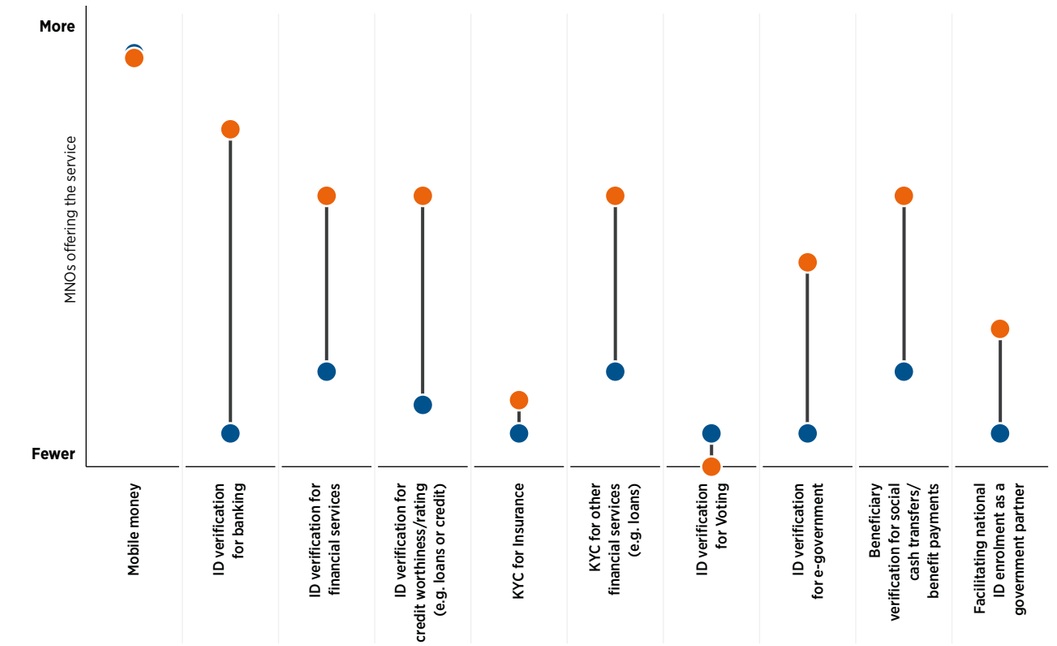


Base: All respondents. Question: Have you targeted customers with personalised mobile services after introducing a SIM registration process?

One digital-ID linked service, mobile money, has only been possible because MNOs were required to comply with KYC regulation. Other digital-ID linked services, however, emerged when MNOs decided to leverage their SIM registration/mobile money KYC assets even more. Aside from the near-ubiquitous use of mobile money, MNOs are offering up to nine identified ID-linked services that leverage their SIM registration and mobile money KYC assets (see Figure 14). The top three ID-linked services launched by MNOs (other than mobile money) are: 1) beneficiary verification for social cash transfers/benefit payments (used during the COVID-19 pandemic); 2) ID verification for financial services; and 3) KYC for financial services, such as loans.

Figure 15

MNOs with ID verification capabilities against a database/smartcard (e.g. government maintained) offer the most use cases, on average



MNOs with a capability to verify customers' ID credentials against a government database/smartcard
MNOs without such capability | Added value of ID verification

Base: MNOs that launched ID-linked services. Question: Have you targeted customers with personalised mobile services after introducing a SIM registration process? Note: The difference between the services offered: shows the added value that ID verification brings to MNOs that have the capability to verify customers' ID credentials against a database/smartcard compared to MNOs without such capability. Based on percentage of respondents. Difference in services offered between the two groups: >64 percentage points

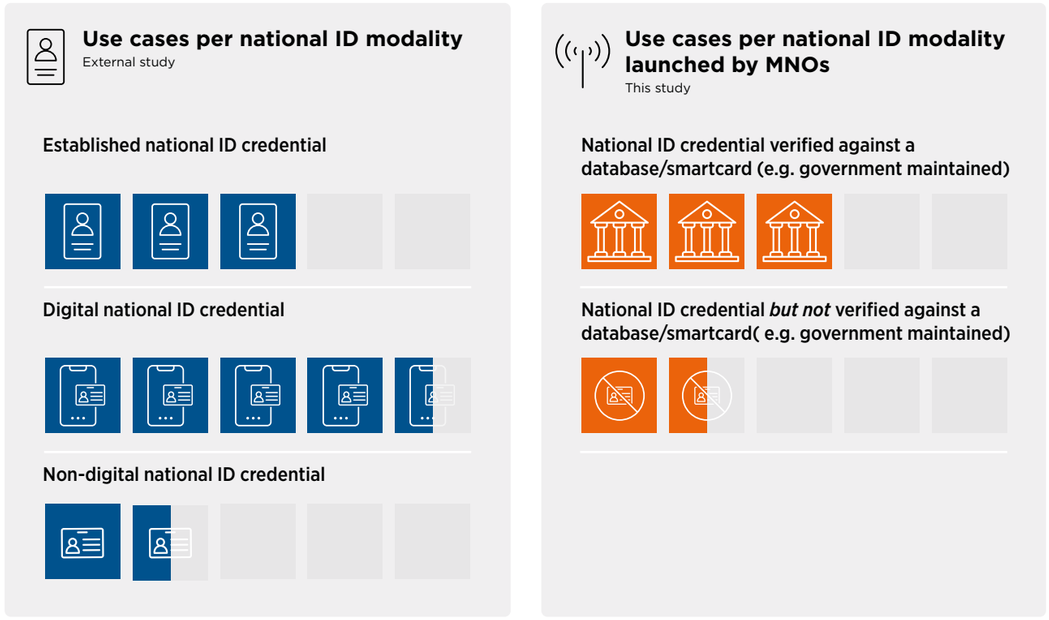
Excluding mobile money services, MNOs that have the capability to verify IDs against a database/smartcard are, on average, twice as likely to have launched mobile-enabled ID-linked services with revenue potential, primarily ID verification for banking (Figure 15) . Those without such capabilities claim to have rolled out only a few services in comparison.

A study by the International Telecommunication Union (ITU),[42] albeit in a different context, associated national ID programmes with certain use cases. For example, a national ID may be used for functional purposes, such as SIM registration, mobile money, digital banking, voter registration, health verification, cash transfers and KYC for various purposes. Similar trends emerge in this study by the GSMA (Figure 16).

42 Benson, C. et al. (2017). Digital Financial Services: Ecosystem. ITU.

Figure 16

Digital ID offers more service opportunities

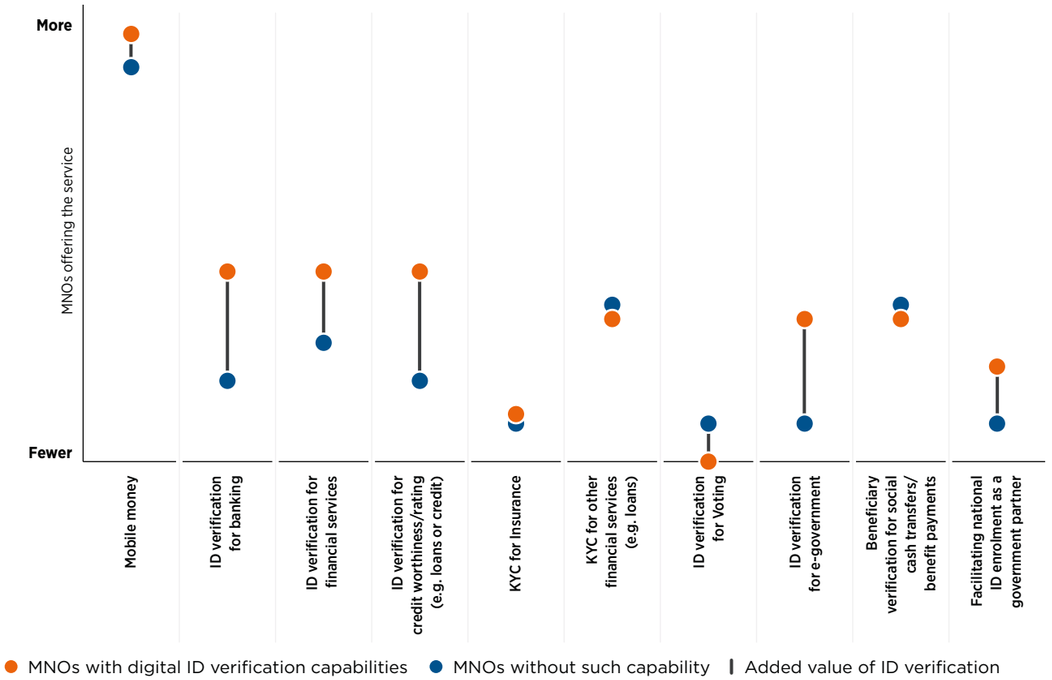


Note: The infographic compares the results of this study with an ITU study. It shows the average number of functional use cases attributed to certain national ID modalities. 'Established' = operational and in use.

The more digital and verifiable an ID verification process is, the more likely an MNO will be to be able to offer value-added services to its identified customers.

Figure 17

MNOs with digital ID verification capabilities are, on average, more likely to offer functional use cases than MNOs without these capabilities



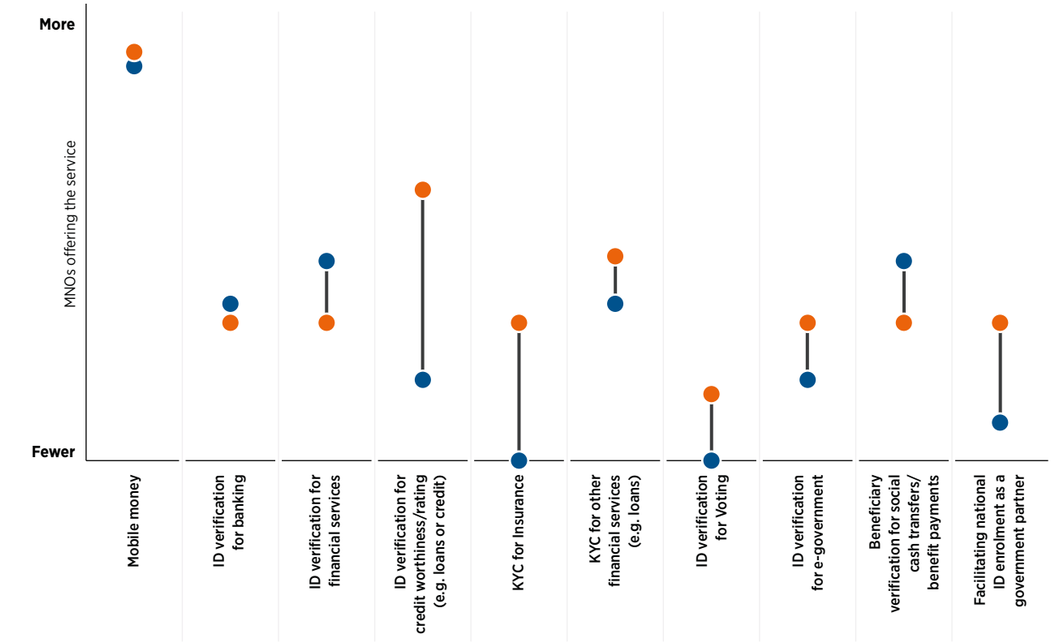
Base: MNOs that launched ID-linked services. Question: Have you targeted customers with personalised mobile services after introducing a SIM registration process? Note: The difference between the services offered: shows the added value that ID verification brings to MNOs that have the capability to verify customers' ID credentials digitally compared to MNOs without this capability. Based on percentage of respondents. Difference in services offered between the two groups: >23 percentage points.

MNOs with digital ID verification capabilities have launched a variety of mobile services, but fewer than MNOs that can verify IDs against, typically, a government-maintained database/civil registry, national ID or similar smartcard (Figure 17). Having digital capabilities made it more likely for MNOs in this study to launch mobile services with revenue-earning potential than MNOs with non-digital/physical ID verification capabilities.

Offering a suite of mobile financial services appears to be the greatest current revenue-earning opportunity for MNOs that are empowered by their government and keen to invest in ID verification capabilities.

Figure 18

More use cases are launched by MNOs that are satisfied with the robustness of their SIM registration and mobile money KYC processes than MNOs that are not



Base: MNOs that launched ID-linked services. Question: Have you targeted customers with personalised mobile services after introducing a SIM registration process? Note: The difference in services offered: shows the added value of ID verification for MNOs that are satisfied with their SIM registration/mobile money KYC processes compared to MNOs that are not. Based on percentage of respondents. Difference in services offered between the two groups: >40 percentage points.

MNOs that are satisfied with the robustness of their SIM registration/mobile money KYC processes are more likely to have launched ID-linked mobile services with revenue-earning opportunities than MNOs that are not satisfied (Figure 18). The services launched most often by these MNOs are ID verification for creditworthiness/ credit ratings, ID verification for financial services (e.g. loans) and KYC for insurance.

Some MNOs improved access (for vulnerable communities) to their existing capabilities, such as beneficiary identification for social cash transfers and KYC for financial services, by relaxing ID verification requirements during the COVID-19 pandemic.

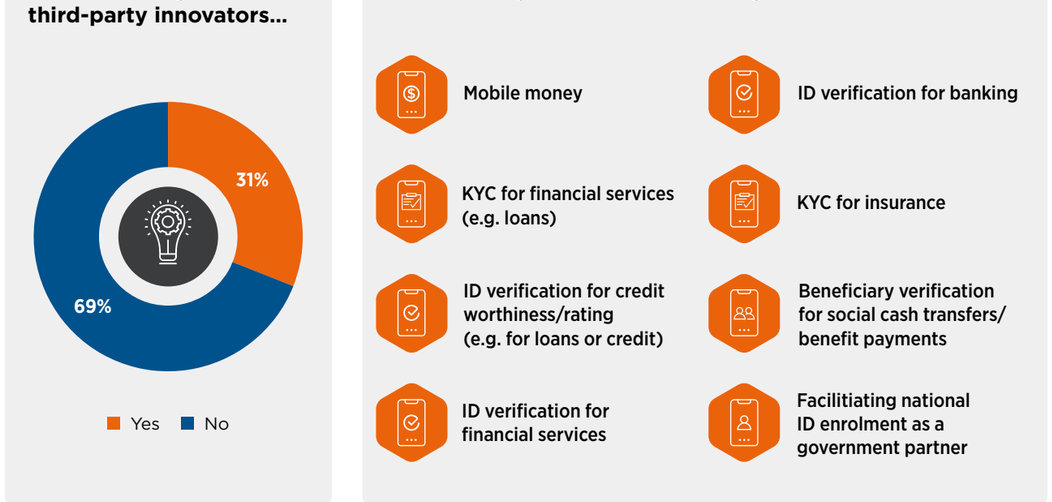
4.2 Current digital ID use cases: partnerships between MNOs and third-party innovators

The ability to innovate and provide digital ID and verification services may lie within an MNO's current capabilities, and several MNOs in this study have launched services on their own. However, there are likely many with less capacity to invest in new digital initiatives outside their core business functions. Here, it would be practical to identify and encourage partnerships with innovative solution providers that have sector expertise, scale and influence across a particular industry. The partners on both sides may be able to benefit from synergies, leveraging each other's core expertise, network and customer base. Such partnerships might also be designed to alleviate concerns relating to storage and management of customer data and regulatory issues including market entry; competition; market dominance and antitrust.

Around a third of MNOs in this study are working with third-party innovators and collectively they have at some stage launched at least 8 different ID-linked services including on-boarding services; ID verification; loans via mobile money; microcredits; savings and G2P transfer services (see Figures 19 and 20). A further 61 percent are willing to work with innovators in future to roll-out novel ID-linked services.

Figure 19

Partnerships are increasing the potential for commercially viable and socially impactful ID services

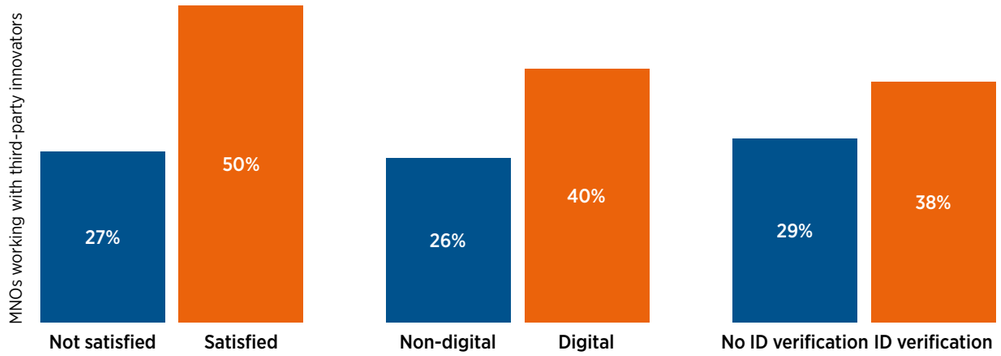


Base: All respondents. Question: Have you targeted customers with personalised mobile services after introducing a SIM registration process? Question: Are you currently working with any third-party innovators to offer any of these mobile services?

Working with partners on digital identity and verification services is one of several paths for an MNO to diversify their service portfolio. With the proliferation of digital services, wider mobile network coverage and increasing use of mobile and smartphones, digital identity is likely to become increasingly important for assuring the authenticity of customers' identity when they access these digital services and reduce criminal activities and fraud. Offering digital identity services can also support the inclusion of underserved populations/new customers and is a business opportunity for MNOs estimated to be growing.[43] In India, Bharti Airtel invested in several small companies that leverage machine learning to improve on-boarding for KYC and customer service.[44,45]

Figure 20

MNOs that are satisfied with the robustness of their SIM registration/mobile money KYC processes and that are digitally sophisticated are more likely to work with third-party innovators



Base: All respondents. Question: Are you currently working with any third-party innovators to offer any of these mobile services? Notes: **'Satisfied' –** MNOs that are satisfied with the robustness of their SIM registration/mobile money KYC processes. **'Not satisfied' –** MNOs that are not satisfied with the robustness of their SIM registration/mobile money KYC processes. **Digital –** MNOs with all digital forms of ID verification. **Non-digital –** MNOs with physical, in-person and perhaps paper-based ID verification capabilities that may involve travel to an agent or retailer. **ID verification –** MNOs with ID verification capabilities against a database/smartcard (e.g. government maintained). **No ID verification –** MNOs without ID verification capabilities against a database/smartcard (e.g. government maintained)

43 Maynard, N. and Morrow, S. (2020). Digital identity: technology evolution, regulatory landscape and forecasts 2020–2025. Juniper Research.
44 Airtel. (3 October 2018). Airtel strengthens Artificial Intelligence portfolio.
45 Airtel. (21 May 2020). To offer the best-in-class service experience to its customers, Airtel acquires strategic stake in Conversational AI focused Startup – Voicezen.

COMMERCIALLY SUSTAINABLE ROLES FOR MOBILE OPERATORS IN DIGITAL ID ECOSYSTEMS

4.3 Current digital ID use cases: SIM registration and KYC processes are being harmonised

Harmonisation, in the context of this study, refers to combining and simplifying SIM registration and mobile money KYC on-boarding processes (where mobile money services are offered) allowing a new customer to typically experience a one-step-process to register for a SIM card and mobile money account/wallet. The benefits of harmonisation include cost and time savings, higher revenues, improved customer satisfaction and avoidance of penalties due to non-compliance.[46,47,48,49]

Across many countries, MNOs recognise that mobile money KYC tends to involve more comprehensive ID and customer due diligence (CDD) requirements compared to SIM registration.

> "Mobile money KYC has more mandatory data than MNO SIM card registration."

> "Mobile money registration requires further information from the client, such as occupation and amount of expected monthly transactions."

Some of the MNOs in this study deploy more digitally sophisticated ID verification methods for mobile money KYC, which might be able to be extended to SIM registration for harmonisation efforts.

> "Mobile money on-boarding and ID-verification is performed online."

> "The ID verification is remote with a query to the government database."

Some MNOs have harmonised.

> "Mobile money on-boarding is the same as SIM-registration."

> "There is no difference."

> "We perform the same validation for mobile SIM registration."

One MNO explained their harmonised process while acknowledging that the ID requirements for mobile money KYC and SIM registration are different.

> "We have introduced one-step registration. Customers who register a SIM card are registered on mobile money and they activate their account by setting a PIN. The KYC requirements for mobile money, in terms of number of accounts allowed and documents allowed for registration, vary from SIM registration in some ways. Customers are allowed two mobile money accounts and a maximum of three SIM cards. Driver's licences are an acceptable document for registration for mobile money, but not for SIM registration, for example."

46 UNHCR. (2019). Displaced and Disconnected.
47 Kipkemboi, K. (2019). Overcoming the Know Your Customer hurdle: Innovative solutions for the mobile money sector. GSMA Mobile Money.
48 GSMA. (2013). The Mandatory Registration of Prepaid SIM Card Users.
49 FATF. (2020). Digital Identity.

Case study 1

ESWATINI

Harmonisation of sim registration and mobile money KYC[51]

Eswatini is a small low-income country in Southern Africa with a predominantly rural population and very high penetration of national ID cards.

The government is committed to increasing financial inclusion. A risk-based, tiered KYC system is used to provide access to basic bank or mobile money accounts for those without certain ID credentials, for example.

By referencing a Memorandum of Understanding between the telecommunications regulator and central bank to collaborate on inclusion measures, Eswatini has been able to harmonise on-boarding requirements for SIM registration and mobile money KYC. The requirements are the same, which means that a customer only needs to go through the KYC process once to enable a SIM card/mobile and open a mobile money account/wallet.

The benefits of harmonisation have included efficiency, interoperability, financial/ digital inclusion and reduced costs.

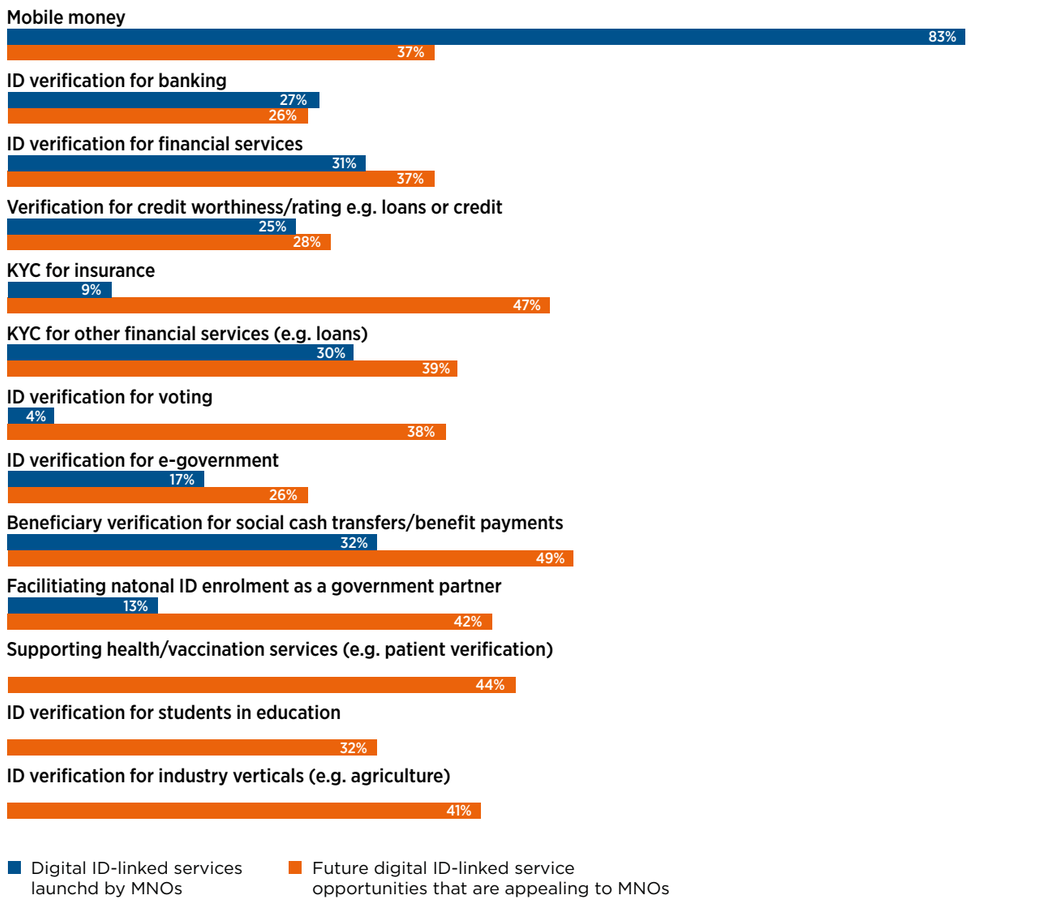
50 AFI (2019), **KYC Innovations, Financial Inclusion and Integrity**.

51 Corley, S. (12 November 2020). **Digital Identity Week 2020 Summary**. Digital Frontiers Institute.

4.4 Opportunities for future digital ID use cases: MNO appetite for new services is high

Figure 21

There is notable MNO interest in developing new commercial ID-linked services



Base: All respondents. Question: Have you targeted customers with personalised mobile services after introducing a SIM registration process and, looking to the future, which mobile services do you find appealing to offer your identified customers? Note: While MNOs in this sample have said they do not currently offer mobile services related to health/vaccinations, education or industry verticals, the GSMA is aware of these services being provided by other MNOs across LMICs.

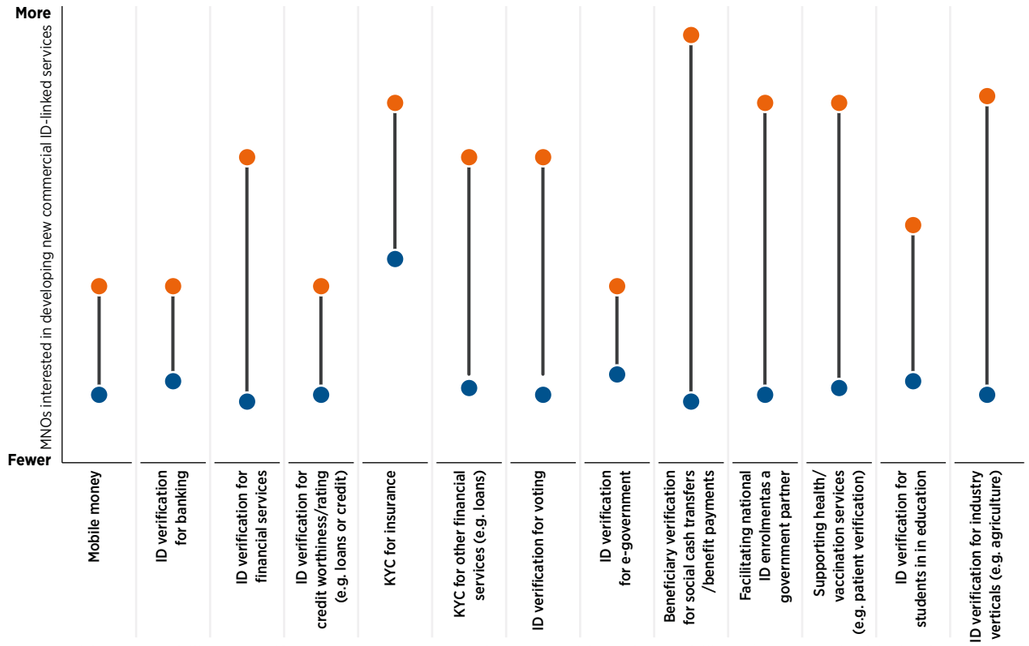
While some MNOs have already launched mobile services for a range of use cases, a higher proportion are interested in launching a greater variety of novel ID-linked use cases in future (Figure 21). KYC for insurance and beneficiary verification services for social cash transfers/benefit payments are the most frequently cited use cases. Less prevalent use cases, including ID verification for health/vaccinations, education and other industry sectors, are also of interest to MNOs.

Opportunities to launch new mobile services might involve consortia or public-private partnerships (PPPs). There are instances, such as in Tanzania, where there have been robust implementations of biometric national ID ecosystems. TANMOA[52] is a consortium in Tanzania that has been encouraged to and helped facilitate the issuance of national IDs through SIM card re-registration drives. A recent example of MNO involvement in national ID drives is in Nigeria where, in December 2020, the National Identity Management Commission licensed MNOs and other private sector partners to act as government enrolment agents, signing up citizens biometrically and linking their ID to their mobile phone number.[53]

Governments may have a broader interest in MNOs providing ID services beyond national IDs. In Kenya, a government-led consortium that includes an MNO is piloting a digital health ID app. In Benin, Kea Medicals[54] (a digital health ID and app) have engaged with the government and worked in collaboration with an MNO to enable identified customers/patients to access their patient records, book appointments remotely by mobile and attend online doctor consultations.

Figure 22

MNOs without ID verification capabilities against a database/smartcard (e.g. government maintained) are particularly interested in launching new ID-linked services



Base: MNOs interested in future ID-linked service opportunities. Question: Looking to the future, which mobile services do you find appealing to offer your identified customers? Note: The difference in interest in future ID-linked service opportunities shows the potential added value of ID verification for MNOs that do not have the capability to verify customers' ID credentials against a database/smartcard (e.g. government maintained) compared to MNOs with this capability. Based on percentage of respondents. Difference between the two groups: >53 percentage points.

52 ID4Africa Livecast. (12 November 2020). Spotlight on Tanzania's Identity Ecosystem.

53 See NIMC: https://nimc.gov.ng/docs/Approved_Data_Capturing_Agents.pdf

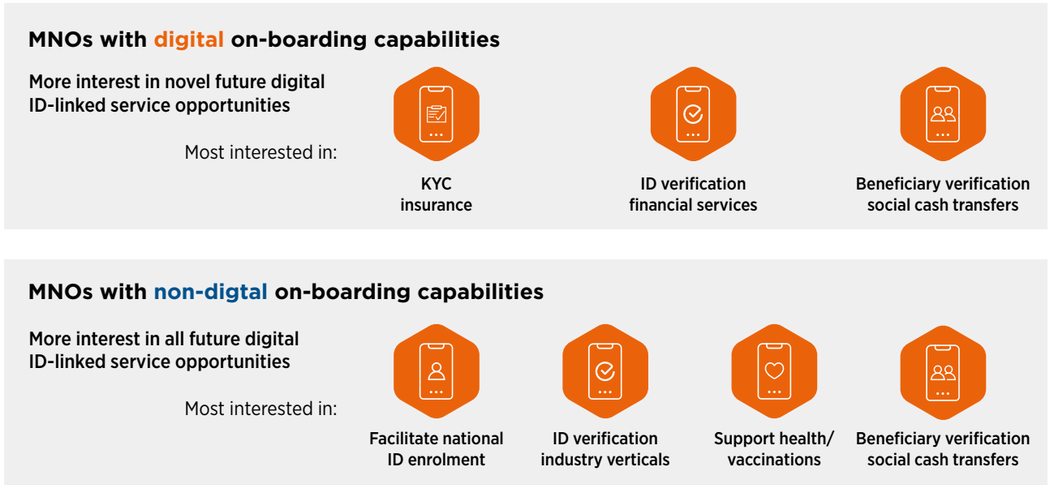
54 Lowe, C. (2020). Benin's Digital Health ID: Providing mobile-enabled healthcare benefits to the underserved – Kea Medicals.

MNOs with ID verification capabilities against a database and/or smartcard are more likely to have already launched mobile-enabled ID-linked services than MNOs without these capabilities. However, these MNOs are still interested in pursuing other service opportunities.

MNOs that do not have the capability to verify IDs against a database/smartcard find future ID-linked services in general even more appealing, especially launching beneficiary verification for social cash transfers, providing ID verification for industry verticals and KYC for insurance, facilitating national ID enrolment and supporting health/vaccination services (see Figure 22).

Figure 23

The most in-demand use cases differ for MNOs with digital and non-digital ID verification capabilities



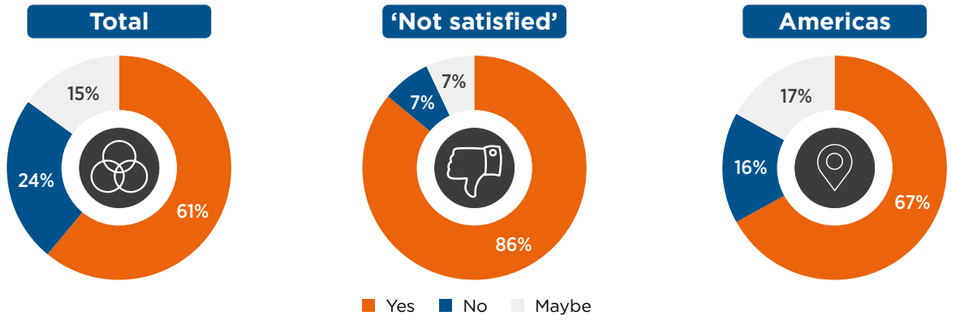
Base: MNOs interested in future ID-linked service opportunities. Question: Looking to the future, which mobile services do you find appealing to offer your identified customers? Note: 'Novel' = service opportunities less prevalent/not yet explored; 'All' = all service opportunities in Figure 22

MNOs with digital ID verification capabilities show more interest in services that are less prevalent or have not already been offered. Conversely, MNOs with non-digital ID verification processes, aside from mobile money, show more interest in all future service opportunities, in some instances, services that have already been rolled out (Figure 23). The latter group appears more willing to support government and citizen-oriented initiatives for digital identity provision, financial inclusion and health.

4.5 Opportunities for future digital ID use cases: working with innovators is appealing

Figure 24

Two-thirds of MNOs are willing to partner with innovators to develop new use cases



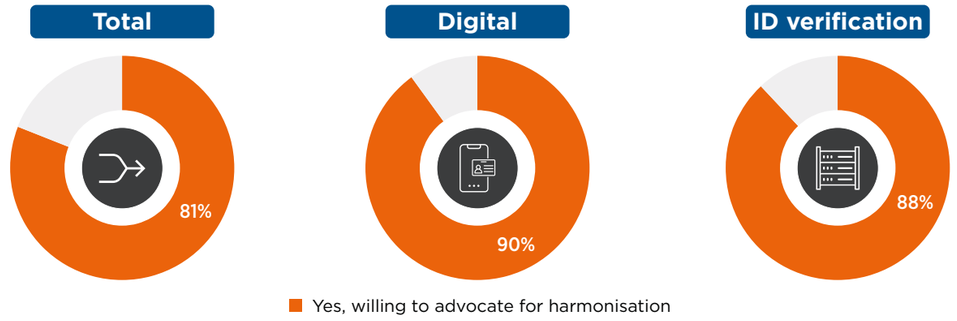
Base: All respondents; MNOs that are not satisfied with the robustness of their SIM registration/mobile money KYC processes; MNOs in the Americas region (including North, Central and South America). Question: In future, would you be willing to work with third-party innovators on new services?

The 61 per cent of MNOs in this study willing to work with third-party innovators were interested in all the ID-linked service opportunities presented to them. They were most interested in KYC for insurance and financial services, and ID verification for health and multiple industry verticals. More MNOs, on average, are willing to work with third parties to innovate in the Americas and among those MNOs who are not satisfied with the robustness of their SIM registration and mobile money KYC processes (see Figure 24).

4.6 Opportunities for future digital ID use cases: most MNOs support harmonisation

Figure 25

Most MNOs are willing to advocate for harmonisation of SIM registration with mobile money KYC



Base: All respondents; MNOs with digital ID verification capabilities; MNOs with ID verification capabilities against a database/smartcard (e.g. government maintained). Question: Would you be willing to advocate to harmonise SIM registration with KYC to offer customers better mobile-linked services, for example, requiring only one visit to register?

Eighty-one per cent of MNOs are willing to advocate to government bodies (telecom and financial regulators) to harmonise their rules for SIM registration and mobile money KYC and empower these MNOs to merge the two processes (Figure 25). This is more prevalent among those with digital ID verification capabilities (90 per cent) and/or those with ID verification capabilities against a database/smartcard (e.g. government maintained) (88 per cent).

Summary

MNOs in this study appear to have launched several ID-linked mobile services, some in partnership with third-party innovators, but those with digital processes seem to have launched twice as many on average. **Offering ID-linked mobile financial services (aside from mobile money) seems to be the greatest current revenue-earning opportunity for MNOs keen to invest in digital ID verification capabilities.**

However, over half of MNOs in this study are dissatisfied with their SIM registration and KYC processes and are willing to invest in verification against a government database/smartcard. This is backed by strong interest in working with innovators; launching new ID-linked mobile services and third-party verification in the future; and willingness to advocate for harmonisation of SIM registration processes with mobile money KYC. There is an opportunity for MNOs to work with partners (including the GSMA), innovators and governments to foster a more conducive environment for launching commercially sustainable and socially impactful mobile services.

5

COSTS

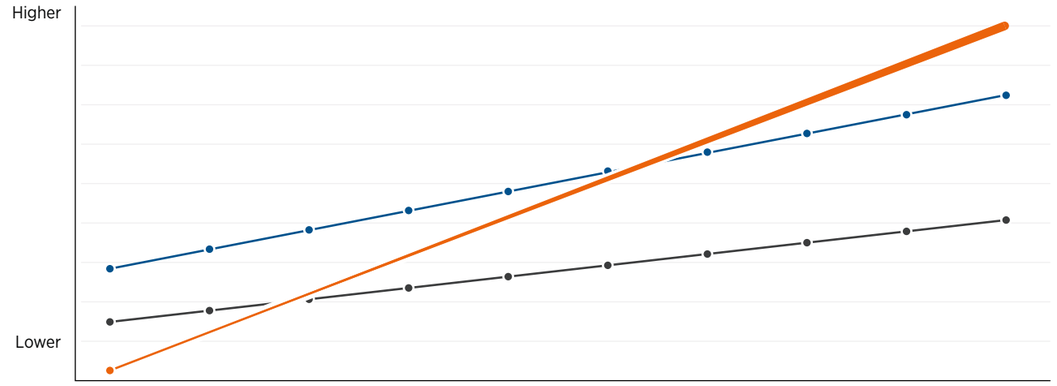
Digital ID verification costs more, but many MNOs predict it will pay off

MNOs that believe their customer ID verification processes are robust tend to have invested more

In general, as governments invest more in the digital transformation of their economies and data protection frameworks, the more MNOs tend to invest in their ID verification processes for SIM registration and mobile money KYC (Figure 26).

Figure 26

With increasing digitisation and where data protection/privacy legislation is more established, MNOs tend to invest more in their ID verification processes



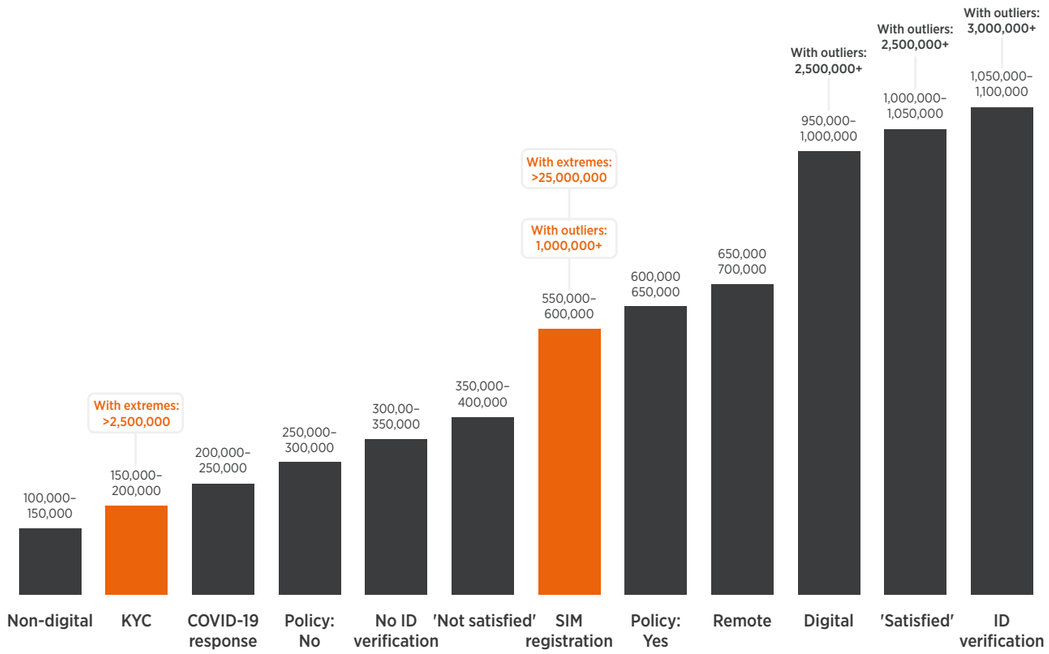
Source: GSMA analysis

MNOs in this study have, on average, 7.2 million unique mobile subscribers (range of about one to 31 million) and an ARPU[55] of about $6[56] (range of about $1 to $28). As a rudimentary benchmark, data from this study suggests that the average overall set-up cost for an MNO's SIM registration and mobile money KYC processes is approximately $0.50 per user.[57] MNOs have invested to varying degrees in their SIM registration and mobile money KYC processes (Figure 27). Investments are generally higher when they are put into increasingly digitised infrastructures that require, for example, robust networks, hardware, software, devices and retail footprints.[58] The greatest investments tend to be in digital processes that verify digital IDs, possibly biometric and usually against a government-maintained database/civil registry or chip-based national ID (smartcard) where the MNO has planned a purposeful and rigorous implementation, perhaps in partnership with the government and/or a consortium of motivated innovators and integrators.

55 Average revenue per user
56 Average unique mobile subscribers and ARPU of all MNOs in this study, excluding the United States. Based on annualised GSMA Intelligence operator data, 2020.
57 Data available from this study is survey and interview-based, and a margin of error should be expected. Data is not intended to be representative of all MNOs nor the countries or regions covered by this research.
58 A detailed comparison of investment costs by the size of MNOs, number of unique subscribers or revenue, for example, has not been included in this study and could be worthy of further research

Figure 27

Investment landscape for MNO SIM registration and mobile money KYC processes (USD)



Base: All respondents. Question: What was your overall cost for setting up SIM registration and mobile money KYC processes? Notes: Figure 27 shows average overall set-up cost (in USD) of an MNO's SIM registration and mobile money KYC processes. Costs in some instances are converted from local currency into USD using exchange rates from OANDA, September 2020. Costs are rounded and provided as a range. Costs, including outstanding outliers and extremes (aggregated), are shown. Costs can include instances where mobile money KYC costs are bundled with SIM registration. **SIM registration –** reflects the average MNO investment in SIM registration as a benchmark against other categories. **KYC –** reflects the average MNO investment in mobile money KYC (KYC costs can be bundled with SIM registration, however). **ID verification –** MNOs with ID verification capabilities against a database/smartcard (e.g. government maintained). **No ID verification –** MNOs without ID verification capabilities against a database/smartcard (e.g. government maintained). **Digital –** MNOs with all digital forms of ID verification. **Non-digital –** MNOs with physical, in-person and perhaps paper-based ID verification that may involve travel to agents/retailers. **Remote –** MNOs with ID verification capabilities, such as the ability to on-board oneself via a mobile phone. **Policy –** 'Yes' or 'No': MNOs in countries either with or without government data protection/privacy legal frameworks. **'Satisfied' –** MNOs that are satisfied with the robustness of their SIM registration/mobile money KYC processes. **'Not satisfied' –** MNOs that are not satisfied with the robustness of their SIM registration/mobile money KYC processes. **COVID-19 response –** MNOs that have responded to COVID-19 by relaxing their on-boarding (e.g. remote, more IDs or tiers)

The average investment in SIM registration set-up for MNOs in this study is estimated to be around $600,000 and rises to over $3 million for those with more digitised implementations. Some invested more, requiring between $5 million and $11 million in overall set-up costs, while some additional implementations were estimated at up to $25 million over several years. Mobile money KYC processes tend to have relatively low investment among MNOs in this study compared to SIM registration. These costs appear to often be subsumed within SIM registration infrastructure and, therefore, may be skewed. However, several MNOs claimed their set-up costs for mobile money KYC reached up to $2.5 million.

In this study, MNOs in countries with established data protection/privacy legal frameworks invest over two times more in their ID verification processes than MNOs in countries where no legislation is in place. There also appears to be a level of investment optimism among MNOs where their host countries are debating and intending to enact such legislation.

Interestingly, the set-up investment in SIM registration and mobile money KYC processes by MNOs that responded to COVID-19 by relaxing their on-boarding requirements, was relatively low. This suggests that these MNOs may not have had robust or highly digitised processes prior to the pandemic, and had to adopt new measures to ensure their customers remained connected to mobile (and were digitally and financially included). These MNOs may have also been more at risk of losing customers and revenue compared to MNOs that had already digitised their processes, minimising contact with customers yet continuing robust customer on-boarding and service during the pandemic.

MNOs that believe they can reap the benefits of digital ID verification invest 250 per cent more

MNOs that believe they will reap the benefits of digital ID verification, such as turning their SIM registration compliance investment into commercial opportunities, tend to invest an average of 250 per cent more in their ID verification processes for SIM registration and mobile money KYC.

MNOs who believe they can realise the benefits of digital ID verification and turn a compliance obligation into an opportunity

Invest on average

250%

more in ID verification processes for SIM registration and KYC

Set-up costs for MNOs deploying digital ID verification capabilities are significantly higher

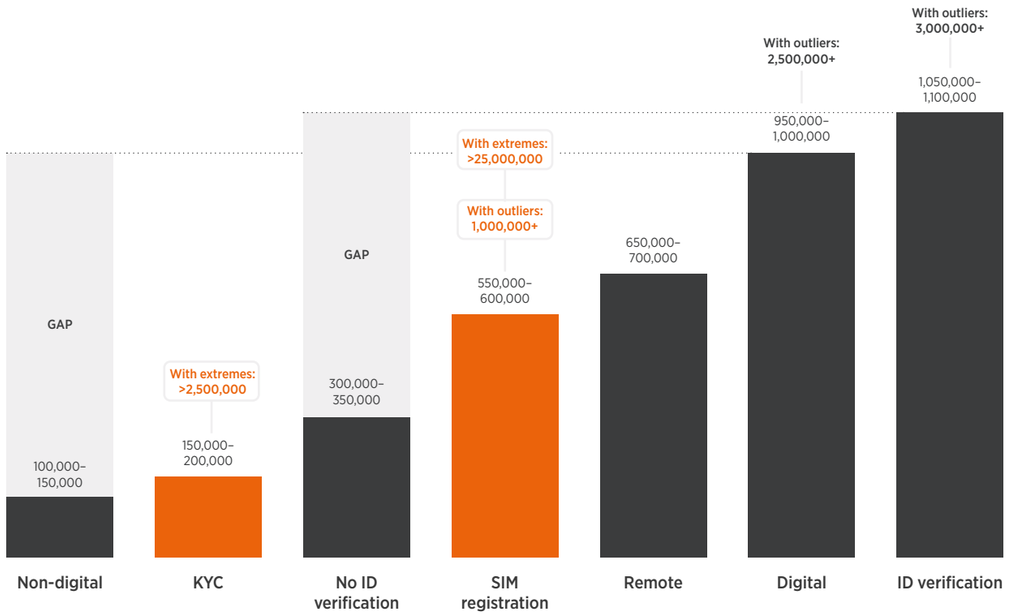
Investment in SIM registration and mobile money KYC differs when the customer on-boarding and ID verification method, such as the use of various digital technologies, is taken into account. Overall set-up costs for SIM registration and mobile money KYC processes involving digital ID verification are over six times higher than for non-digital processes (Figure 28).

Set-up costs are higher for SIM registration and mobile money KYC processes with ID verification against a database/smartcard (e.g. government maintained) than processes that capture digital IDs in general, and over three times higher than those without ID verification against a database/smartcard.

MNOs in this study that deployed remote ID verification processes had incurred set-up costs approximately four times higher than those incurred by MNOs with non-digital processes.

Figure 28

MNOs with digital ID verification capabilities during customer on-boarding invest significantly more than those without



Base: All respondents

The level of MNO investment in SIM registration and mobile money KYC processes is directly correlated with how robust they perceive these processes to be

MNOs that indicated they were 'satisfied' with the robustness of their SIM registration and mobile money KYC processes tend to invest, on average, around two times more in setting up these processes (Figure 29). The investment gap widens to 2.5 times when compared with MNOs that are 'not satisfied'. Satisfied MNOs can include those with digital, non-digital and ID verification capabilities (typically against a government-maintained database/smartcard).

Conversely, MNOs that are not satisfied with the robustness of their processes invest about a third less on average, and almost two-thirds less than MNOs that are satisfied.

Figure 29

MNOs that are satisfied with the robustness of their SIM registration and mobile money KYC processes tend to invest about two times more, on average

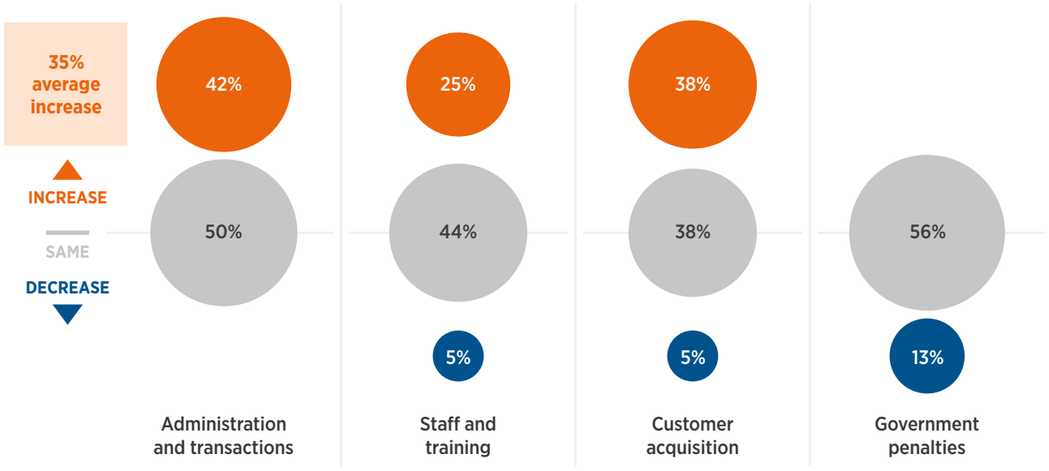
Base: All respondents

Some MNOs have seen their operating costs rise since implementing SIM registration processes

Following the imposition of SIM registration and mobile money KYC mandates in countries that required it, MNOs incurred capital (CAPEX) and operating expenditure (OPEX) to set up the relevant processes to fulfil customer ID verification requirements. Since these processes were rolled out, MNOs in this study reported an average overall cost base increase of 35 per cent (Figure 30). These MNOs cited cost increases in administration and transactions (42 per cent of MNOs), customer acquisition (38 per cent) and staff and training (25 per cent). There is some anecdotal evidence to suggest that some MNOs achieved some cost reductions.

Figure 30

Investment in SIM registration processes has increased some MNOs' operating costs by up to 35 per cent



Base: MNOs reporting cost base fluctuations since implementing SIM registration processes. Question: How have your costs changed since introducing SIM registration and KYC? Note: Bubbles represent the percentage of MNOs reporting cost base fluctuations since introducing SIM registration processes

Some MNOs indicated where they have seen changes to their cost base:

> The validation process for SIM registration has been in place for many years and the fee paid to the validation authority is increased every year according to the Consumer Price Index (CPI).

> KYC costs increased by 25 per cent due to the need to hire telemarketing and go-to-market personnel.

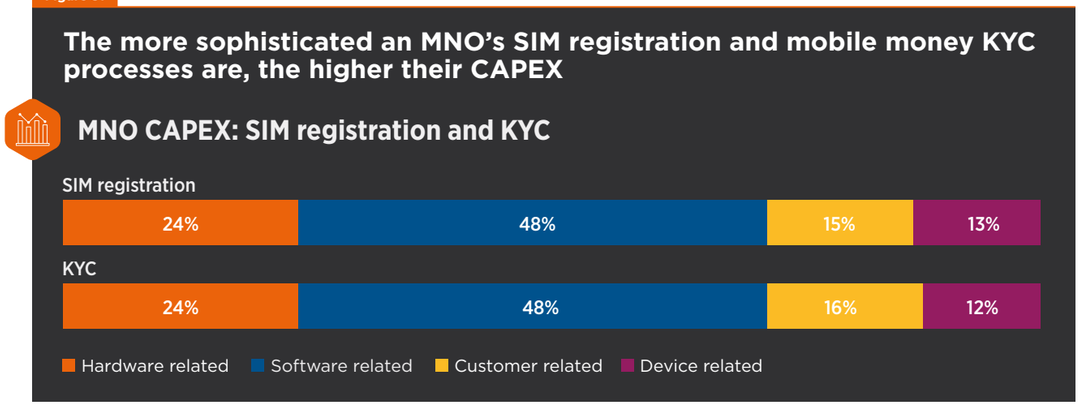
> There has been recruitment of around two million customers per year since the identification of subscribers and, as part of their on-boarding, we are charged by the ID authority around 70 cents per customer on-boarded.

> With KYC implementation, administrative and transaction costs increased from practically nothing to over $2,500 monthly [for a subscriber base of over 2.5 million].

5.1 Capital expenditure

Figure 31

The more sophisticated an MNO's SIM registration and mobile money KYC processes are, the higher their CAPEX



Base: All respondents. Question: What was your estimated CAPEX to set up your SIM registration and KYC processes? Notes: **Hardware related –** e.g. IT backbone, computers, servers, network (centrally located equipment, telecoms network, etc.). **Software related –** e.g. data platform (software, apps, etc.) **Customer related –** e.g. retailers, agents, training, customer activation-related assets and initial expenditure. **Device related –** e.g. portable scanners and devices.

More digitally sophisticated SIM registration and mobile money KYC processes require higher hardware-related CAPEX

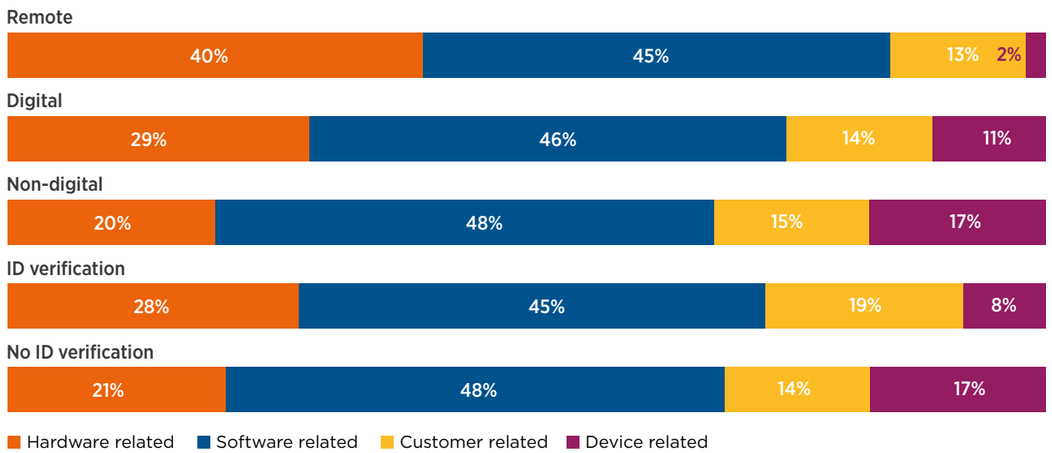
As MNOs' SIM registration and mobile money KYC processes become more digitally sophisticated, they appear to be progressively investing proportionally more CAPEX (see Figures 31 and 32) in hardware-related elements (e.g. supporting the IT backbone, computers, servers, network). Software and customer-related investments (e.g. data platform and retailers, agents, training, customer activation-related assets) remain broadly similar. While initial spend on devices may be high for MNOs with more digitally sophisticated ID verification processes, proportionally it is low for those deploying remote on-boarding, which may be driven by the ability to self-on-board at home, for example.

Two digitally sophisticated processes, remote on-boarding (e.g. ability to on-board oneself via a mobile phone) and ID verification against a database/smartcard, stand out for comparison. MNOs employing remote on-boarding require less customer-related expenditure (e.g. retailers, agent footprint) and fewer portable devices in the field, which is reflected in their lower proportional expenditure. MNOs verifying ID credentials against databases/national smartcards, however, require higher customer-related expenditure and modern digital ID scanners or biometric terminals.

Interestingly, the proportion of CAPEX spent on hardware-related elements for MNOs with remote on-boarding is double that of MNOs with non-digital on-boarding/ID verification.

Figure 32

More digitally sophisticated customer ID verification processes have higher hardware-related CAPEX



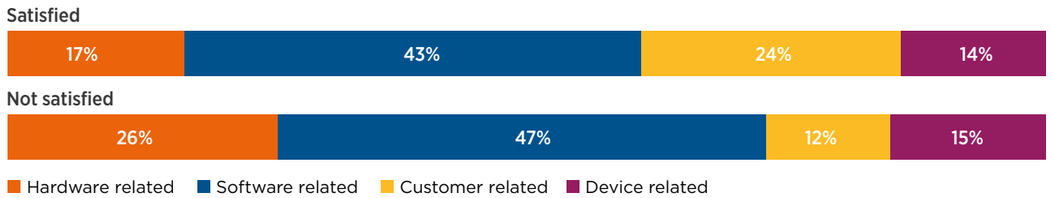
Base: All respondents. Question: What was your estimated CAPEX to set up your SIM registration and KYC processes? Notes: **Remote –** MNOs with ID verification capabilities, such as the ability to on-board oneself via a mobile phone. **Digital –** MNOs with all digital forms of ID verification. **Non-digital –** MNOs with physical, in-person and perhaps paper-based ID verification that may involve travel to agents/retailers. **ID verification –** MNOs with ID verification capabilities against a database/smartcard (e.g. government maintained). **No ID verification –** MNOs without ID verification capabilities against a database/smartcard (e.g. government maintained)

MNOs satisfied with their SIM registration and mobile money KYC processes invest more in customer-related assets

MNOs that are satisfied with the robustness of their SIM registration and mobile money KYC processes invest proportionally more CAPEX in customer-related assets (e.g. retailers, agents, training, customer activation-related assets and initial expenditure) and less in hardware- and software-related assets compared to MNOs that are not satisfied (Figure 33). The increased MNO focus on, for example, retail and agent footprint and customer service activities, and any subsequent effect on customer satisfaction, may be driving higher satisfaction with ID verification/on-boarding processes.

Figure 33

MNOs reporting they are 'satisfied' with their SIM registration and KYC process implementations invest more in retail, agent and customer-related assets

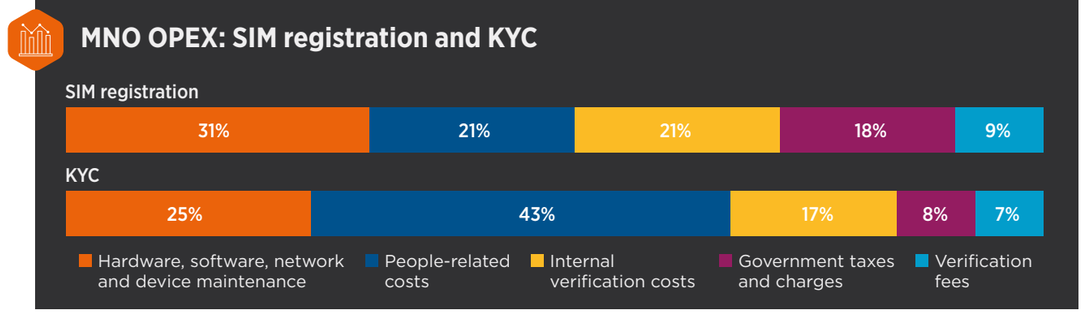


Base: All respondents. Question: What was your estimated CAPEX to set up your SIM registration and KYC processes? Notes: **'Satisfied' –** MNOs that are satisfied with the robustness of their SIM registration/mobile money KYC processes. **'Not satisfied' –** MNOs that are not satisfied with the robustness of their SIM registration/mobile money KYC processes

5.2 Operating expenditure

Figure 34

MNOs' operating expenditure for mobile money KYC is focused largely on people



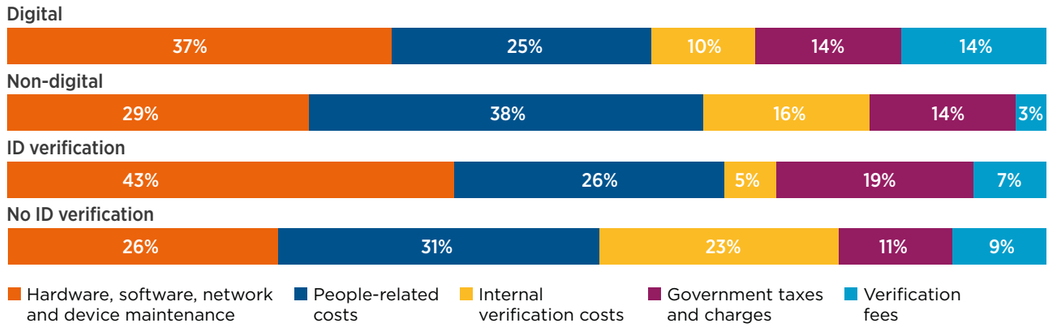
Base: All respondents. Question: What is your estimated OPEX per year for your SIM registration and KYC processes? Notes: **Hardware, software, network, device maintenance** – e.g. maintenance of servers, network, data platform, replacement devices, scanners, etc. **People-related costs** – e.g. on-going staff, retailer, agent, customer and training costs. **Internal verification costs** – e.g. internal costs related to verifying customer IDs and customer on-boarding. **Government taxes and charges** – e.g. SIM tax and other government charges. **Verification fees** – e.g. verification fees (charges per query, or alternative frequency, to a government database)

The digital sophistication of MNOs' SIM registration processes is inversely proportional to the OPEX spent on people

As MNOs' SIM registration/mobile money KYC processes become more digitally sophisticated, people-related OPEX decreases proportionally, while maintenance of hardware, software, network and devices and government charges and verification fees increase (see Figures 34 and 35).

Figure 35

People-related operating costs decline as SIM registration and KYC processes become more digitally sophisticated



Base: All respondents. Question: What is your estimated OPEX per year for your SIM registration and KYC processes? Notes: **Digital** – MNOs with all digital forms of ID verification. **Non-digital** – MNOs with physical, in-person and perhaps paper-based ID verification that may involve travel to agents or retailers. **ID verification** – MNOs with ID verification capabilities against a database/smartcard (e.g. government maintained). **No ID verification** – MNOs without ID verification capabilities against a database/smartcard (e.g. government maintained)

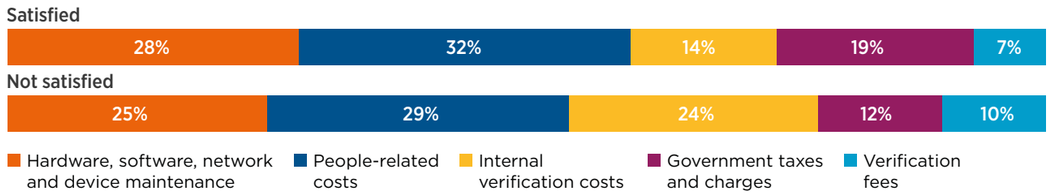
MNOs satisfied with the robustness of their SIM registration and mobile money KYC processes spend less on internal verification costs

MNOs that are satisfied with the robustness of their SIM registration and mobile money KYC processes spend proportionally more OPEX on taxes and government charges (Figure 36). More robust processes, which are typically more digitally sophisticated, can bring greater transparency and accountability and allow for tax collection. There may, therefore, be a benefit for governments to facilitate ID verification for MNOs as this might lead to higher tax revenue.

Conversely, satisfied MNOs spend less on internal verification costs, perhaps reflecting their ability to better comply with regulation (through digital customer ID verification or against a database, for example) or more frictionless customer ID verification processes. MNOs that are not satisfied with the robustness of their SIM registration and mobile money KYC processes spend more internally verifying customers' details.

Figure 36

MNOs reporting they are 'satisfied' with the robustness of their SIM registration and mobile money KYC processes spend less on internal verification costs

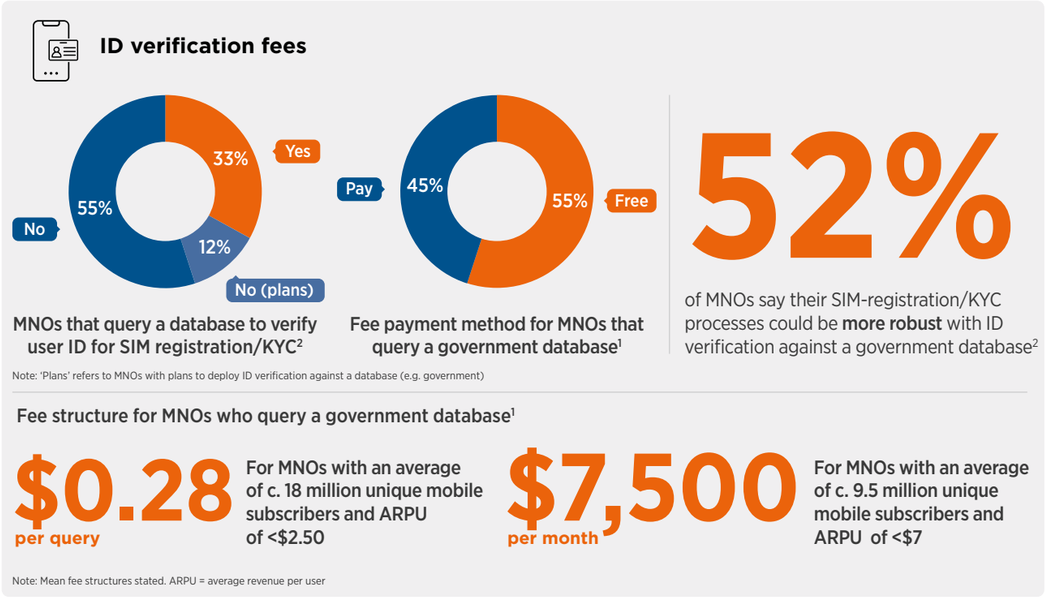


Base: All respondents. Question: What is your estimated OPEX per year for your SIM registration and KYC processes? **'Satisfied'** – MNOs that are satisfied with the robustness of their SIM registration/mobile money KYC processes. **'Not satisfied'** – MNOs that are not satisfied with the robustness of their SIM registration/mobile money KYC processes

5.3 ID verification fees

Figure 37

A third of MNOs verify IDs by querying a database/smartcard while over half say their ID verification could be more robust if they had this capability



Base: 1 = MNOs that query a government database to verify user IDs for SIM registration/KYC; 2 = All respondents. Question: Do you query a government database to verify a user's ID during SIM registration? Question: How much do you pay per query? Question: Do you have a cost-sharing agreement with the government/regulator for ID verification?

Around a third of MNOs in this study verify IDs against databases/smartcards (e.g. government maintained) (Figure 37). There are also several implementations in progress among other MNOs surveyed. The benefits are well known,[59] and there is a clear drive from MNOs to comply with regulation, as well as demand for commercial ID-linked mobile services that can stimulate inclusion. The CAPEX and OPEX an MNO incurs as part of complying with customer ID verification requirements can have an impact their financial position when these costs cannot be easily recouped. However, such investments are increasingly seen as necessary to building and maintaining a robust ID verification ecosystem based on SIM and mobile money registration, and could be leveraged to support access to a plethora of life-enhancing services that may not have been attainable in the past.

59 Wilson, M. and Waddington, R. (2019). Understanding capture and validate KYC processes: global experiences, challenges and learnings. GSMA.

From the outset, there is an opportunity for all stakeholders involved in an ID verification implementation to discuss partnerships, cost sharing and incentives that can benefit the government, the private sector and customers.[60,61] Without careful planning, implementations could fail. Various MNOs conducting ID verification against databases/smartcards are not satisfied with the robustness of their available ID verification processes, but those that are satisfied tend to invest more in building out their infrastructure to leverage this capability.[62]

Fifty-two percent of MNOs in this study report that their ID verification could be more robust against a government-maintained database/smartcard. They generally demonstrate willingness to invest in digital transformation, although many appear to have been held back in the past. This trend is supported by recent research with MNOs globally,[63] which found that 75 per cent have accelerated digital transformation due to COVID-19, and 74 per cent plan to increase their digital investments, citing the benefits of reduced costs, improved customer experience and increased revenue. However, in the Middle East and across Africa, only about one in three MNOs have prioritised the shift to digital, and in Latin America only one in four.

Another source of concern for MNOs considering digital transformation is the conflicting political, social and commercial interests of public institutions. These can result in delays to ID verification infrastructure and realising the associated benefits.[64]

> “ Our country’s SIM registration law is not implemented yet. This law was approved recently, however, the country’s ID authority has to grant access for the validation of customers’ information and is reluctant to do so. Therefore, the telecommunications regulatory authority has been negotiating with them for access. The main issue is that ID verification queries shall be free, however, the ID authority wants to charge for it. Before COVID-19, both authorities were discussing this matter, but for now this matter has a lower priority.

Summary

The upfront costs (CAPEX) required for MNOs to invest in SIM registration and mobile money KYC processes tend to increase with more robust and digitised implementations, particularly for MNOs that believe they can reap the benefits of digital ID verification. More robust processes are correlated with launching more revenue-earning use cases and more future opportunities, and have potential to digitally and financially include more customers. There is an opportunity for MNOs, where necessary, to seek partnerships with innovators or work in a consortium to pool expertise in the delivery of more robust verification and on-boarding processes. Governments may be able to facilitate, and provide the financial and cost-sharing incentives and conducive regulation that promote data protection and market competition.

60 Amin, M. and De Koker, L. (12 November 2019). “A Vision for Collaborative Customer ID Verification in Africa”, CGAP Blog.
61 CGAP. (August 2019). Beyond KYC Utilities: Collaborative Customer Due Diligence.
62 Clark, J. et al. (2019). Identity authentication and verification fees: overview of current practice. The World Bank ID4D.
63 Upstream and TIC. (2021). The road to digital: How telcos are migrating from physical to digital to broaden revenue in 2021 and beyond.
64 Cooper, B. et al. (2018). Biometrics and financial inclusion: A roadmap for implementing biometric identity systems in sub-Saharan Africa. CENFRI.

COMMERCIALLY SUSTAINABLE ROLES FOR MOBILE OPERATORS IN DIGITAL ID ECOSYSTEMS

6 THREATS

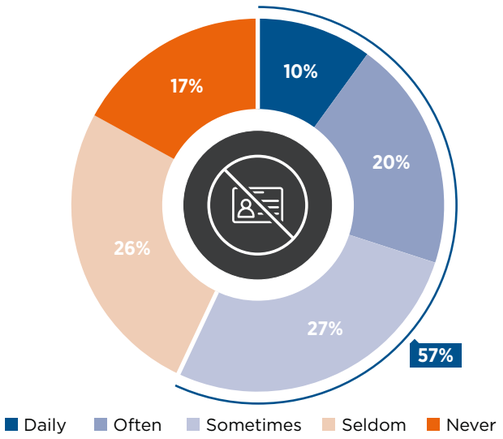
Robust customer ID verification is still a challenge for many MNOs

MNOs in this study identified several issues and threats related to ID verification within their SIM registration and mobile money KYC processes.

6.1 Inability to on-board customers to SIM registration and KYC due to lack of required ID

Figure 38

57 per cent of MNOs are regularly unable to on-board customers



Customers are still regularly unable to complete SIM registration or mobile money KYC because they lack the required ID.

Reasons cited for this include: expired ID, lost ID, no digital ID card, forgotten ID, fake ID and copied ID.

Base: All respondents. Question: How often are you unable to on-board customers because they lack the required ID?

Although various MNOs in this study are able to digitally verify customer IDs, 64 per cent tend to have more problems on average on-boarding customers who lack the required ID (Figure 39). A quarter of MNOs with digital ID verification capabilities appear unable to on-board customers because they do not have the required digital ID, which may be due to not having a digital ID card, relying on a family member or friend to register for them, not being allowed to register or not seeing the value of having their SIM card registered against a verifiable ID in their own name. Geographically, MNOs in Sub-Saharan Africa claim to experience more regular customer on-boarding issues due to lack of required ID.

Figure 39

MNOs in some contexts experience more customer on-boarding issues

64% of MNOs with digital ID verification capabilities

AND

79% of MNOs in Sub-Saharan Africa

claim they are regularly unable to on-board customers due to lack of required ID

Base: MNOs with digital ID verification capabilities; MNOs in Sub-Saharan Africa. Question: How often are you unable to on-board customers because they lack the required ID? Note: 'Regularly' includes combined MNO responses to: 'daily', 'often' and 'sometimes' unable to on-board customers to SIM registration and mobile money KYC due to lack of required ID

MNOs with more digitally sophisticated SIM registration and mobile money KYC processes experience fewer issues on-boarding customers since they verify IDs against a database/ smartcard and/or rely on remote on-boarding.

MNOs with more digitally sophisticated SIM registration and mobile money KYC processes, including remote on-boarding and ID-verification against a database/ smartcard (e.g. government maintained), tend to experience fewer on-boarding issues (Figure 40). Interestingly, MNOs that improved their digital on-boarding capabilities during the COVID-19 pandemic also appear to have fewer on-boarding issues.

Figure 40

MNOs with digitally sophisticated ID verification processes experience fewer on-boarding issues

>60% of MNOs with digitally sophisticated ID verification capabilities

claim they experience fewer customer on-boarding issues due to lack of required ID

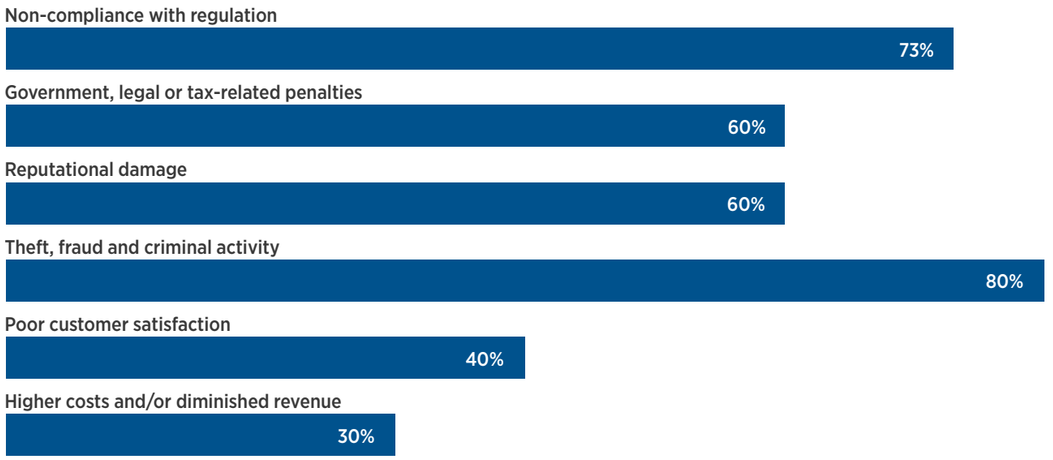
Base: MNOs with digitally sophisticated on-boarding capabilities use remote on-boarding capabilities and verify IDs against a database/smartcard (e.g. government maintained). Question: How often are you unable to on-board customers because they lack the required ID?. Note: 'Fewer customer on-boarding issues' includes combined MNO responses to: 'seldom' and 'never' unable to on-board customers to SIM registration and KYC due to lack of required ID

6.2 Perceived threats when validating IDs for SIM registration and mobile money KYC

Criminal activity (80 per cent) and non-compliance with regulation (73 per cent) are the top two perceived threats for MNOs that validate IDs for SIM registration or KYC purposes.

Figure 41

The main threats to MNOs when validating IDs for SIM registration and mobile money KYC processes are criminal activity and regulatory non-compliance



Base: All respondents. Question: What threats do you perceive when validating IDs for SIM registration or KYC purposes?

Theft, fraud and criminal activity and non-compliance with regulation were the most-cited risks for MNOS when validating IDs during SIM registration and/ or KYC (Figure 41). This concern is supported by the frequent imposition of fines on MNOs that, for example, are unable to maintain accurate customer identification details on their databases.[65] However, these inaccuracies may be caused by a lack of robust official identification made available to the population. Cyberattacks on mobile telecom accounts and mobile financial transactions are also on the rise, compromising data and risking the reputations of MNOs. For example, one MNO was subject to a lawsuit claiming losses from a SIM-swapping[66] attack, highlighting the potential liability of MNOs for criminal activities.[67]

MNOs pointed out the potential threats posed by customers and agents:

> SIM registration and KYC are also essential as customers and agents become more sophisticated in crimes such as fraud, anti-money laundering (AML) and cybercrime.

65 GSMA. (2016). Mandatory registration of prepaid SIM cards: Addressing challenges through best practice.

66 A form of identity theft in which the attacker convinces an MNO to port a victim's phone number to a different device. The attacker can then attempt to gain access to the victim's financial accounts and personal information.

67 Lexis Nexis. (2019). ThreatMetrix Q2 2018 Cybercrime Report.

While non-compliance with regulation is considered a major threat, MNOs pointed out that unclear regulations and different understandings and implementations of regulations between stakeholders and institutions can lead to non-standardised implementation.

> [There are] profound differences in the understanding and implementation of the legislation…multiple meetings did not make it possible to standardise either the understanding nor the implementation.

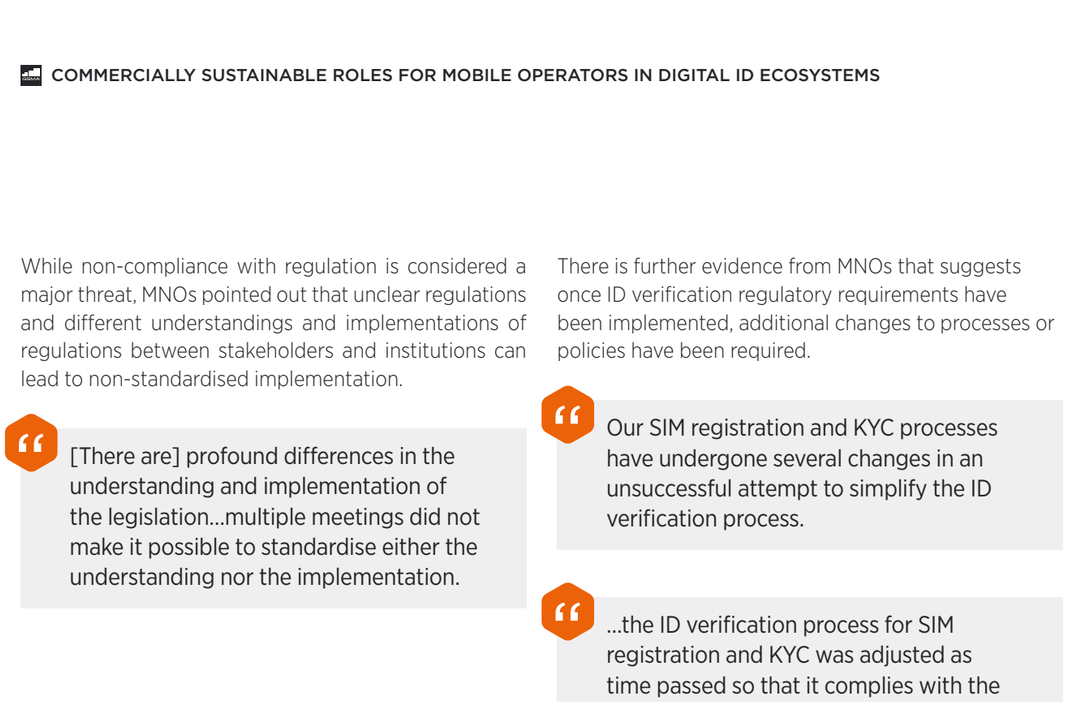
There is further evidence from MNOs that suggests once ID verification regulatory requirements have been implemented, additional changes to processes or policies have been required.

> Our SIM registration and KYC processes have undergone several changes in an unsuccessful attempt to simplify the ID verification process.

> …the ID verification process for SIM registration and KYC was adjusted as time passed so that it complies with the necessary legislation.

Figure 42

MNOs with digitally sophisticated customer ID verification processes perceive fewer threats from SIM registration and KYC regulations



Base: All respondents. Question: What threats do you perceive when validating IDs for SIM registration or KYC purposes? Notes: **ID verification** – MNOs with ID verification capabilities against a database/smartcard (e.g. government maintained). **Digital** – MNOs with all digital forms of ID verification. **Non-digital** – MNOs with physical, in-person and perhaps paper-based ID verification that may involve travel to agents/retailers.

MNOs with digital ID verification processes perceive fewer threats when verifying IDs for SIM registration and mobile money KYC than those with non-digital processes (Figure 42). MNOs with ID verification capability against a database/smartcard perceive even fewer threats.

These same MNOs were also significantly less likely to perceive threats of government penalties, reputational damage, crime and poor customer satisfaction. This appears to suggest that MNOs are satisfied with government ID verification methods and are more confident that they are robust.

MNOs with digital ID verification capabilities perceive the greatest threat as non-compliance with regulation. This could be because digital methods provide more transparency and make full compliance more difficult, especially since not all MNOs can verify IDs against databases (e.g. government maintained) or smartcards.

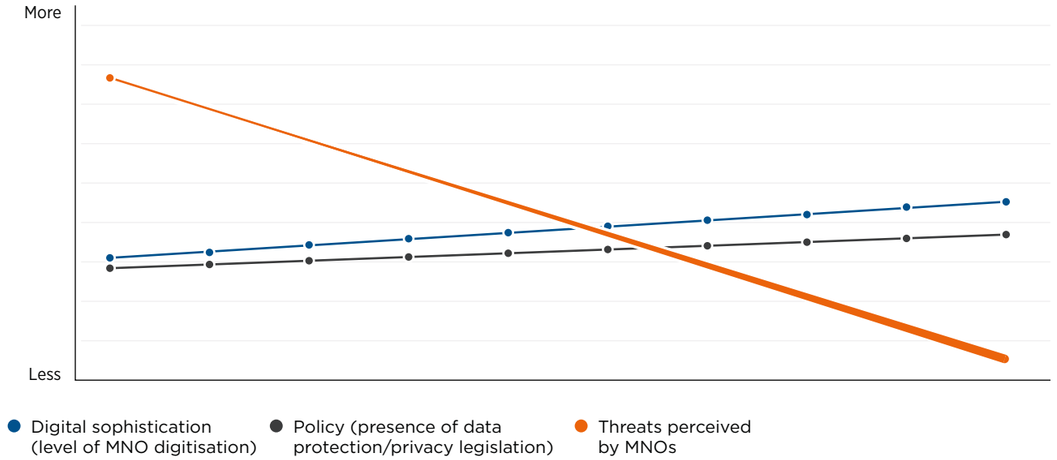
MNOs that verify IDs against databases/smartcards are, relatively, most concerned with higher costs and/or diminished revenue related to ID verification. This suggests that more robust digital implementations could bear significant CAPEX and OPEX that might be difficult to recoup.

6.3 Data protection and privacy

In general, MNOs perceive fewer threats when they use more digital methods of ID verification for SIM registration and mobile money KYC. They also perceive fewer threats when operating in countries where established data protection and privacy frameworks are in place (Figure 43).

Figure 43

MNOs perceive fewer threats when they use digital ID verification for SIM registration and KYC processes and when established data protection and privacy frameworks are in place

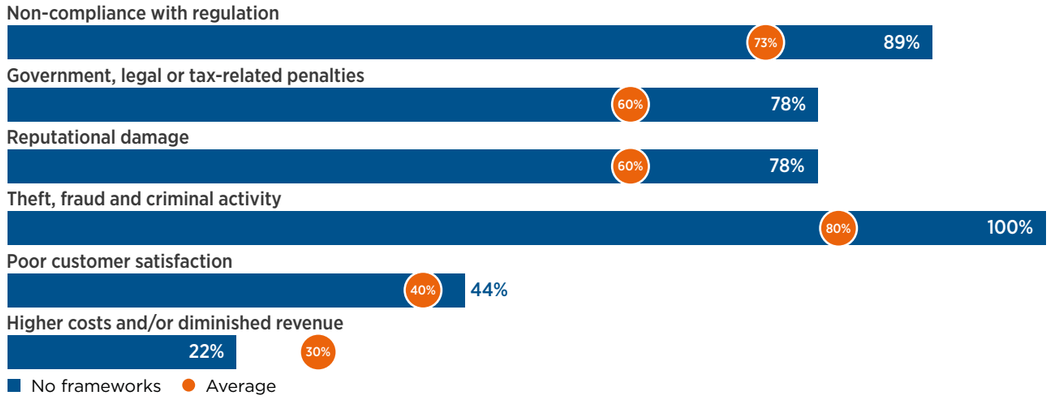


Source: GSMA analysis

MNOs in countries with no data protection and privacy legislation appear to perceive more threats than other MNOs in this study in general (Figure 44).

Figure 44

MNOs perceive more threats when there are no data protection and privacy frameworks



Base: All respondents. Question: What threats do you perceive when validating IDs for SIM registration or KYC purposes? Notes: **No frameworks** – refers to MNOs operating where there are no identified data protection and privacy frameworks. **Average** – all respondents

MNOs are improving the security of their new mobile ID-linked services

The implementation of effective and proportional SIM registration and KYC regulatory frameworks usually involves balancing several conflicting demands. On one side, supporting national security, preventing crime, verifying customer identities in a robust manner and implementing solutions swiftly. On the other side, upholding citizens' rights, including vulnerable and underserved citizens, ensuring a frictionless customer on-boarding experience and maximising social, digital and economic benefits. Robust data protection and privacy are important for building consumer trust in SIM registration processes and any subsequent ID-linked mobile services.

Given that, MNOs in this study were primarily concerned with the threat of non-compliance with regulation; the consequences of subsequent penalties, fees or taxes; and fraud, theft and criminal activity. All MNOs appear to take customer data protection and privacy seriously, and to comply with legislation, including when they develop new ID-linked services.

> They will be applied as required by regulations that govern us.

> There is always strict compliance with the protection of personal data of customers, in any service that is provided, either at present or in the future.

> Services related to identity in general, and that of customers in particular, are strictly regulated.

In cases where local data protection and privacy laws are not deemed sufficient or additional assurances are considered necessary, MNOs may apply stricter measures.[68]

> We have different, strengthened practices.

> There are always additional controls with financial systems and SIM distribution.

68 For example, MNOs may apply stricter measures and protections, such as those outlined by the EU's General Data Protection Regulation (GDPR).

Case study 2

INDIA

India rules against compulsory Aadhaar ID verification by the private sector, influencing verification costs and highlighting an individual's right to privacy and choice in disclosing their identity[69,70]

A court ruling on the constitutionality of Aadhaar ID verification in 2018 highlights the risk of ID verification being unconstitutional and infringing on the human rights of citizens and their data protection and privacy. This is relevant to any country or organisation operating or implementing biometrics and/or verifying ID credentials against a central government database/smartcard for mandates such as SIM registration and mobile money KYC.

Aadhaar is the predominant national form of identity (ID) in India, a 12-digit unique identity number (UIN) for Indian nationals and passport holders. It is voluntary and based on a person's biometric and demographic data. It is the world's largest biometric ID system.

From 2012 to 2018, Aadhaar was the subject of a legal challenge submitted to India's Supreme Court. The challenge was that Aadhaar infringes upon the fundamental rights guaranteed by the Indian Constitution. A verdict was reached which upheld the constitutional validity of the Aadhaar scheme, stating the Aadhaar Act does not violate one's right to privacy when one agrees to share biometric data.

The Aadhaar system can be used to access public services and benefits, although the private sector is not allowed to make it compulsory for accessing services. SIM registration processes, for example, were prohibited from using the Aadhaar system for customer verification and authentication. Alternative forms of identification had to be found instead, such as a voter ID card or driving licence. The Aadhaar Amendment Bill now allows mobile operators to use the Aadhaar system for SIM registration, but they must legally obtain permission from customers. When the Aadhaar system is used for digital verification of customer IDs during KYC/e-KYC, it is estimated to lower ID verification costs considerably compared to other methods (e.g. paper-based).

69 See: **https://dot.gov.in/sites/default/files/29-09-2020.pdf?download=1**

70 Pisa, M. and Woodsome, J. (7 February 2019). **Overcoming the "Know Your Customer" Hurdle with E-KYC.** Center for Global Development.

6.4 Other issues cited by MNOs highlight the complexity of ID verification processes

While there is no consistent or common digital ID-based SIM registration process, MNO respondents pointed to several challenges they encounter when operationalising their processes. Policymakers should therefore consider these challenges when updating their SIM registration and KYC regulations. MNOs should also consider these challenges when engaging their respective governments in consultations on SIM registration and KYC policies.

Figure 45

Other issues and threats MNOs face when validating IDs during SIM registration and KYC

Software

- Software downtime; and
- Difficulty adjusting technical solution to legislation and plans

Data

- Incomplete user data;
- False user data;
- Outdated user data;
- Data corruption from coding/encoding;
- Data cleansing delays; and
- Delays updating customer details.

ID

- Expired IDs;
- Forgotten/lost IDs;
- Using fake or copied IDs;
- Unacceptable IDs;
- Lack of uptake of biometric IDs;
- Illegible IDs; and
- ID photo unusable.

Policy and process

- Different understandings of legislation;
- Multiple changes to national identification process;
- SIM registration adjustments over time to comply with legislation; and
- Error-prone change request process and delays.

Stakeholders

- Different understandings of implementation; and
- Non-attendance at implementation meetings.

Customer

- Rejection process due to regulation; and
- Poor customer satisfaction due to the above.

Note: these issues and threats reflect categorised responses from MNOs in this study

MNOs cited other issues, as well (Figure 45). Implementation of national ID verification is a significant undertaking that can lead to costs, issues and delays if it is not well-planned and implemented.[71]

In instances when digital and/or biometric IDs are required by law for ID verification purposes, such as during SIM registration/KYC, there is a risk of large-scale exclusion of both citizens and non-citizens who have not been able to obtain the new required ID. Failure to consider existing legislation or develop new conducive policies can also lead to the unintended exclusion of citizens, non-citizens, refugees or internally displaced persons (IDPs) from accessing the required ID and accessing life-enhancing services provided through SIM registration and KYC.

> The [population majority] do not have biometric documents imposed by legislation.

> The requirement for a biometric card excludes the majority of regional nationals.

> The requirement of biometrics contravenes existing legislation requiring foreigners living in our country be provided with identification documents issued by their country of origin or their consular representation.

Summary

While MNOs with more digitally sophisticated ID verification processes perceive fewer threats overall, the majority of MNOs identify some threats in the context of their SIM registration and mobile money KYC processes. The main ones are non-compliance with regulation and theft, fraud and criminal activity. MNOs are also regularly unable to on-board customers who lack the requisite identity credentials, although this tends to be less of an issue for MNOs with digital and more robust ID verification. Where data protection and privacy laws are not in place or not robust, MNOs have sometimes enhanced their data protection and privacy practices, going above and beyond what is required in a national context to build and maintain the trust of their customers. Here, there is an opportunity for policymakers to engage with MNOs to better understand this situation and consider appropriate regulation to protect citizens and businesses.

71 Clark, J. (2017). The state of identification systems in Africa: A synthesis of country assessments. The World Bank.

7

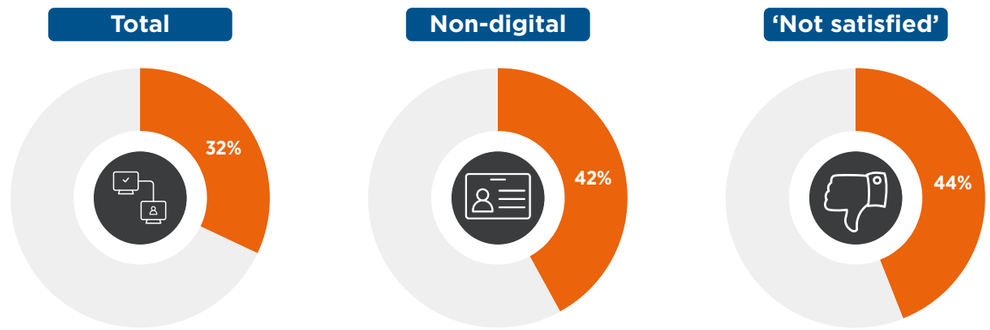
COVID-19

SIM registration and KYC have been relaxed and remote ID verification plans have been accelerated

The sudden onset of COVID-19 ushered in rapid changes to the mobile telecommunications industry, with citizens and businesses around the world accessing and using mobile communications more than ever before. However, it is those in LMICs who depend on this infrastructure most for social and financial inclusion, and MNOs have responded with numerous initiatives to include more customers and citizens despite restrictions on movement, affordability and other challenges.

Figure 46

Around a third of MNOs have relaxed ID verification criteria in response to COVID-19

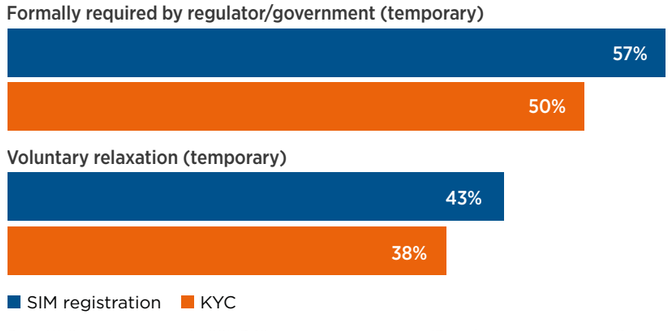


Base: All respondents; MNOs without digital ID verification capabilities; MNOs that are not satisfied with the robustness of their SIM registration/mobile money KYC processes. Question: In response to COVID-19, have you relaxed on-boarding/verification criteria for SIM registration and KYC?

Thirty-two per cent of MNOs in this study have relaxed their on-boarding/ID verification criteria since the onset of COVID-19 (Figure 46). There was a higher prevalence of relaxations among MNOs without digital ID verification capabilities and among MNOs that are not satisfied with the robustness of their ID verification processes. These MNOs may have had to take more steps to assure on-boarding due to less digitised or robust registration processes and infrastructure.

Figure 47

Most ID verification relaxations in response to COVID-19 are temporary mandates

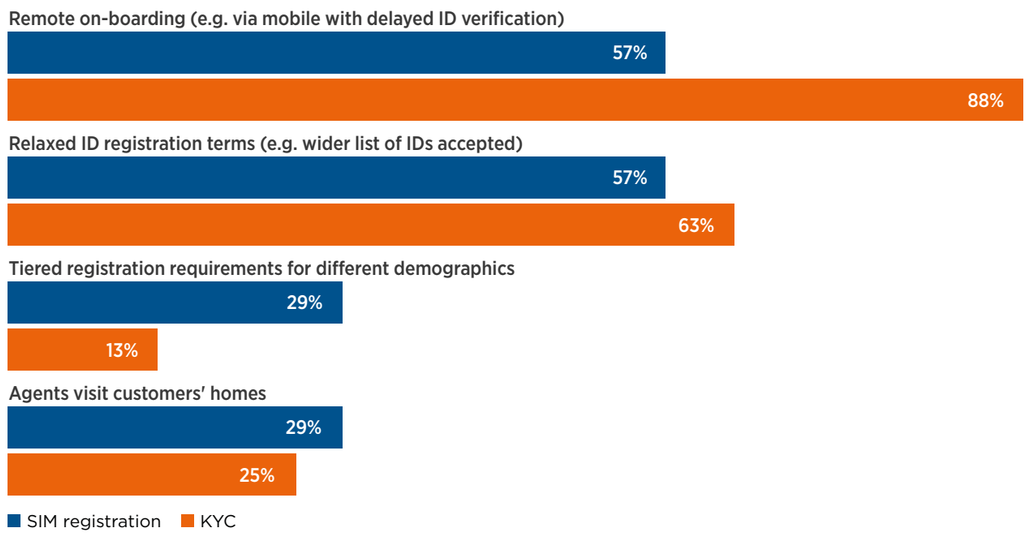


Base: MNOs that responded to COVID-19 by relaxing on-boarding/ID verification requirements. Question: In response to COVID-19, have you relaxed on-boarding/ verification criteria for SIM registration and KYC?

Most relaxations (>57 per cent) are temporary government requirements, but a proportion of MNOs claimed to have initiated temporary voluntary measures to assure on-boarding and provide access to new and existing customers (Figure 47). A minority of measures are claimed to be long term, highlighting some potential cases that could support more long-term regulatory and process reform, and promoting the inclusion of citizens who typically face barriers accessing ID or mobile.

Figure 48

Around two-thirds of MNOs that responded to COVID-19 by relaxing ID verification criteria allowed remote on-boarding or accepted a wider range of IDs



Base: MNOs that responded to COVID-19 by relaxing on-boarding/ID verification requirements. Question: What are the relaxed measures?

Around two thirds of MNO respondents relaxed their ID verification for SIM registration and KYC, enabling remote on-boarding (providing ID details over the phone) and accepting a wider range of IDs, which could be presented over an extended period (Figure 48). There were also various instances of tiered on-boarding (risk-based) in which different levels of CDD were conducted for different types of mobile money accounts, for example. There were also various instances where MNO and mobile money agents visited the homes of customers or potential customers to assist with on-boarding and ID verification efforts.

> The time to certify ID documents was extended.

> The suspension period for unidentified SIMs was extended to six days.

> Allowed to sell SIM cards, swap SIMs and create mobile money wallets with an expired national ID.

Remote customer on-boarding is now more prevalent due to: 1) policy changes in the response to COVID-19; 2) digital benefit payments; and 3) providers recognising the importance of financial inclusion and their customers' need to regularly transact.

More MNOs in this study are using remote ID verification for SIM registration (15 to 28 per cent) and for mobile money KYC (16 to 44 per cent).

> Applied remote access to facilitate data verification.

> Mobile money self-registration via user's phone.

MNOs in this study using digital ID *and* remote ID verification for mobile money KYC increased from 60 to 72 per cent since the COVID-19 pandemic began.

Summary

As a result of the restrictions imposed during the COVID-19 pandemic, various MNOs were permitted to relax their ID requirements for SIM registration and mobile money KYC on-boarding. These relaxations have not only demonstrated their ability to facilitate access to mobile services for underserved and isolating consumers,[72] but also accelerated the digital transformation plans of some MNOs.

There is an opportunity for MNOs and policymakers to take stock of digital ID-led transformations and progress during COVID-19 and consider whether there is a case for making these longer-term changes. Some countries have already legislated to make digital transformations during COVID-19 longer term as they offer potential benefits for MNOs (subscribers, services, competition and revenue), governments (inclusion, revenue, tax, economy) and citizens (digital and financial inclusion).

72 Lowe, C. et al. (2021). Digital identity: accelerating financial inclusion during a crisis. GSMA.

8

Conclusion and recommendations

COMMERCIALLY SUSTAINABLE ROLES FOR MOBILE OPERATORS IN DIGITAL ID ECOSYSTEMS

It is evident that mandatory proof-of-identity requirements for prepaid SIM registration and mobile money KYC are having significant influence on MNOs' customer on-boarding processes. While MNOs have adopted various methods (both physical and digital) to comply with these requirements in the 157 countries where they are mandatory, there appears to be an emerging trend towards adopting more digital processes. This is combined with increasing expectations that MNOs verify, rather than just capture, their customers' identity credentials.

This study has found that these trends pose threats to MNOs' established business models and their ability to comply with the relevant regulations in full, but also offer opportunities to create more robust on-boarding processes that can help MNOs develop more personalised, sustainable and socially impactful services. These opportunities can only be fully realised when governments invest in a robust, inclusive and accessible digital ID ecosystem that caters to the needs of vulnerable and underserved communities, and is supported by appropriate policy and regulatory frameworks that engender trust.

Importantly, digitisation of ID verification also offers a path to social, digital and financial inclusion. SIM registration and mobile money KYC can act as a barrier to individuals who lack the requisite proof of identity. With around a third of MNOs in this study harmonising SIM registration with mobile money KYC or developing digital ID verification processes, and a notable increase in more relaxed ID verification methods, such as remote on-boarding during the COVID-19 pandemic, barriers are being broken down. MNOs have accelerated their efforts to include previously underserved groups, gaining potential new customers and the opportunity to design and tailor revenue-earning services to different demographics that need them most.

This research reveals that MNOs are well-positioned to offer leadership in the digital ID space, leveraging their SIM registration and KYC assets, network reach, customer base with high mobile penetration, trustworthy reputation and ability to reach poor and rural communities. They are also well placed to partner with governments to facilitate the enrolment of individuals in new national digital ID ecosystems, which will ultimately provide a plethora of life-enhancing services to SIM-registered customers. MNOs are also well positioned to provide VaaS to other businesses, particularly in the financial services sector where they can offer a high level of assurance that a mobile user's identity matches the intended user of a third-party service.

Recommendations

The insights from this research, combined with the GSMA Digital Identity programme's experience leading several related initiatives,[73] have informed the following recommendations for MNOs and governments to accelerate their digital transformation plans.

Recommendations for MNOs

Compliance risk: Digital identification and verification against a Government-maintained database or digital ID smartcard/token can lower compliance risk for MNOs. It can also empower them to offer new value-adding services to previously underserved customers.

Market context: MNOs would benefit from considering their local country context when designing new digital ID-linked services, including smartphone adoption, digital literacy, gender gap in digital and financial inclusion, customer access to recognised ID documents, the ability to verify their authenticity, etc.

Data protection, privacy and trust: It is important that MNOs, individually or collectively, advocate to government for the development and enforcement of relevant frameworks. Where policies are still outstanding, it is recommended that MNOs apply strong measures, such as guidelines and processes adopted at the group level, that foster customer trust in digital ecosystems.[74]

Partnering for innovation: It may be beneficial for MNOs to identify, encourage and connect with potential partners/third-party innovators for digital identification and verification services.

Consortia: Given the costs, issues and potential of commercial and digital inclusion opportunities, it is recommended that MNOs seek government and/or ICT industry partners for implementations.

Regulatory harmonisation: Harmonisation of SIM registration and mobile money KYC processes could lead to efficiencies, cost savings and opportunities for digital use cases and the inclusion of customers and citizens. It is recommended that MNOs advocate for conducive policies and regulator collaboration.

Digitisation: It is recommended that MNOs seek to implement robust, considered digital SIM registration/mobile money KYC processes and advocate for the importance of querying customer identification credentials against databases/smartcards (e.g. government maintained), ensuring that redundancies are built in for offline environments, alternative forms of identification, basic/feature phones and environmental shocks.

Digital ID-linked use cases: It will be important to clarify with local partners the specific use cases that digital identification or verification can support, especially innovative services launched during the COVID-19 pandemic. The local context and customer needs should be considered.

73 The programme facilitated MNO-led digital ID initiatives in several countries, including Pakistan, Zambia, Benin, Kenya, Somalia, Tanzania, Sri Lanka, Fiji, Nigeria and others.

74 GSMA (2017). Safety, privacy and security across the mobile ecosystem.

COMMERCIALLY SUSTAINABLE ROLES FOR MOBILE OPERATORS IN DIGITAL ID ECOSYSTEMS

Recommendations for governments

Public-private partnerships (PPPs): Governments investing in digital transformation and digital ID ecosystems should seek to collaborate with mobile and ICT industry partners in upcoming registration or ID verification implementations or improvements.

Incentive schemes: Current SIM registration and mobile money KYC regulation imposes significant costs for MNOs. Consideration of alternative and assistive financial mechanisms is recommended.

Cost-sharing initiatives: Due to the high costs borne by MNOs for SIM registration and KYC compliance, particularly where biometric modalities are involved, mechanisms for sharing costs in PPPs, consortia or otherwise should be considered.

Social and financial inclusion: Conducive regulation (e.g. tiered KYC risk-based policies) should be considered to reduce barriers for citizens to obtain legal proof of identity and access mobile services.

Security and market competition: Conducive regulation could be considered to ensure customers build and maintain trust in digital ecosystem service providers (e.g. MNOs), enabled through robust data protection and privacy legislation. With these frameworks in place, further consideration should be given to promote healthy market competition and the ability of MNOs to launch digital ID use cases given the acceleration of governments' digital transformation plans during the COVID-19 pandemic.

Appendices

Methodology

Desk research and literature review: The first phase of this project involved desk research to explore the overall context, particularly in LMICs. This generated insights in several areas: (i) the identity and digital identity landscape; (ii) the SIM registration and mobile money KYC landscape; (iii) the costs and issues associated with ID verification, SIM registration and KYC; (iv) the regulatory landscape for SIM registration, KYC, data protection and privacy; and (v) the digital ID-linked and verification services landscape and the role of MNOs within this landscape.

Primary research with MNOs: With the assistance of desk research, an in-depth survey was developed to conduct primary research among a sample of senior stakeholders occupying positions in regulatory, governance and legal departments at MNOs in 31 countries. Respondents also included stakeholders in other departments able to answer relevant questions, including IT, strategy, finance and accounting, propositions and sales.

In some instances, surveys have been translated into English from the local language of the country surveyed, and any local currencies have been converted into US dollars. Here, it is possible that additional interpretation of responses was required. In general, responses have been anonymised and aggregated, and monetary references aggregated and provided as ranges for confidentiality purposes.

Respondents to the survey were self-selected depending upon business willingness to participate. The results reflect the answers provided by respondents to the survey. Self-selection, multiple respondents and respondent interpretation of, and willingness or ability to answer questions fully, introduce an element of bias and margin of error. Therefore, the research is not, and not intended to be, representative of nations, regions or MNOs per se. Rather, it is a contribution to the digital identity landscape and the MNOs within it. Caution should be taken when considering the results for extrapolation purposes.

Glossary

Digital sophistication – A categorisation of different methods of on-boarding customers for SIM registration and/or mobile money KYC. Categories range from physical on-boarding and handling of ID or documents (less sophisticated) to more digital forms of on-boarding which, in some instances, could be done without being physically present, for example, at an agent (more sophisticated).

Harmonisation – Combining and simplifying separate SIM registration and mobile money KYC customer on-boarding processes, which allows a new customer to undergo only one process to register for a SIM and a mobile money account/wallet.

ID-linked mobile services (use cases) – Services that are accessible via a mobile phone that require the digital verification of one's identity. For ease and speed of access to mobile services, identity verification could, for example, be completed using details/tokens captured during SIM registration or mobile money KYC. Mobile services could include e-government services, health services, access to medical records, voting, insurance, loans, social cash transfers or industry-specific services for smallholder farmers.

ID verification – A process of checking the validity of, for example, a new customer's legal proof of identity/credential and ensuring they are who they say they are. This may involve a variety of digital and non-digital methods, such as verification of physical IDs by an MNO agent, and using digital ID cards, biometric readers or mobile phones and devices to check against civil registries/databases or check against tokens stored on a smartcard.

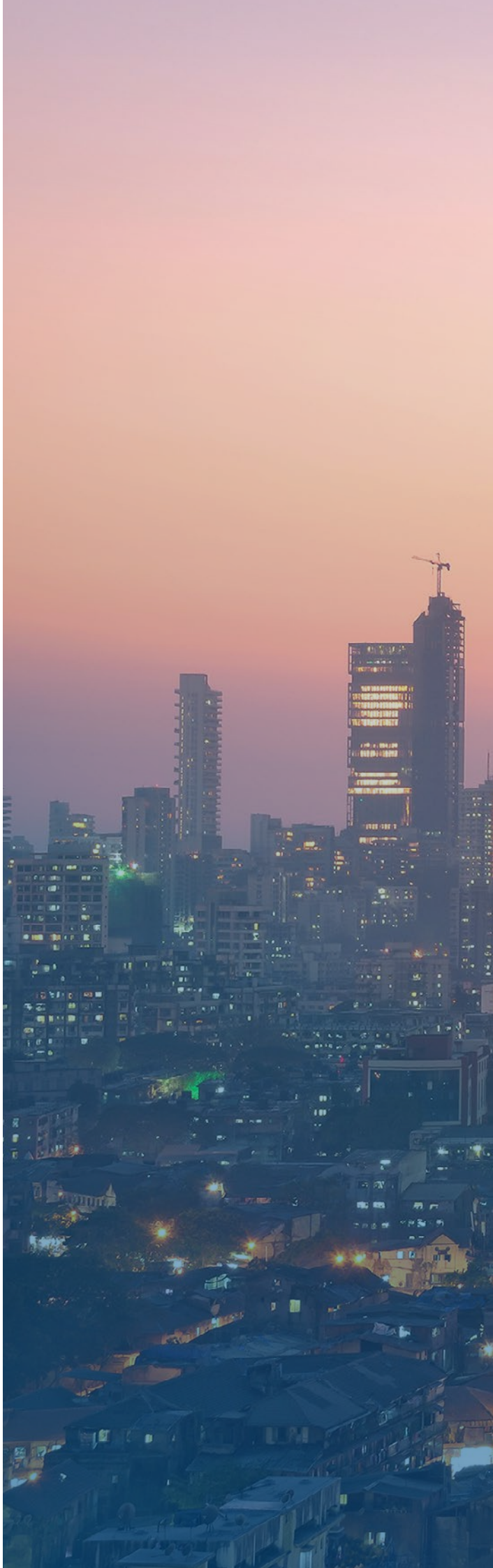
ID verification fees – For SIM registration or KYC, fees are charged for each query to a (usually) government-maintained database to, for example, verify a new customer's identity against their legal identity stored on the database. The fees are often charged by governments to the private sector (in this study, MNOs).

Know Your Customer (KYC) – In a financial services context, a process that requires organisations, to varying degrees, to verify the identity, suitability and risk of new customers applying for an account or mobile wallet. This is a mandatory regulatory requirement in many countries falling within the context of AML/CFT regulation set by central banks and the Financial Action Task Force (FATF).

SIM registration – The process of acquiring, registering and activating a SIM card. In countries with mandatory regulation, this may involve providing forms of officially recognised identification. Many governments have introduced mandatory registration for prepaid SIM card users, primarily as a tool to counter terrorism and money laundering and support law enforcement. The regulation is often set by telecommunications regulatory authorities.

Theft, fraud and criminal activity – Theft is, for example, a criminal stealing one's identity details, ID credential, device, SIM card, IMEI number or phone number. Fraud can involve, for example, SIM swap attacks in which a customer's mobile account is hacked by criminals who may then be able to access personal details, bank accounts and other information. Criminal activity can relate to, for example, terrorism or the financing of terrorism.

Tiered registration requirements – Different tiers of on-boarding requirements for different types of mobile money accounts, for example. During the COVID-19 pandemic, basic mobile money accounts were created with limited functionality and capped transaction amounts. These may require less rigorous customer due diligence compared to other accounts. In some cases, they could be opened on the basis of SIM registration details.



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