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

Contents

Introduction

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).

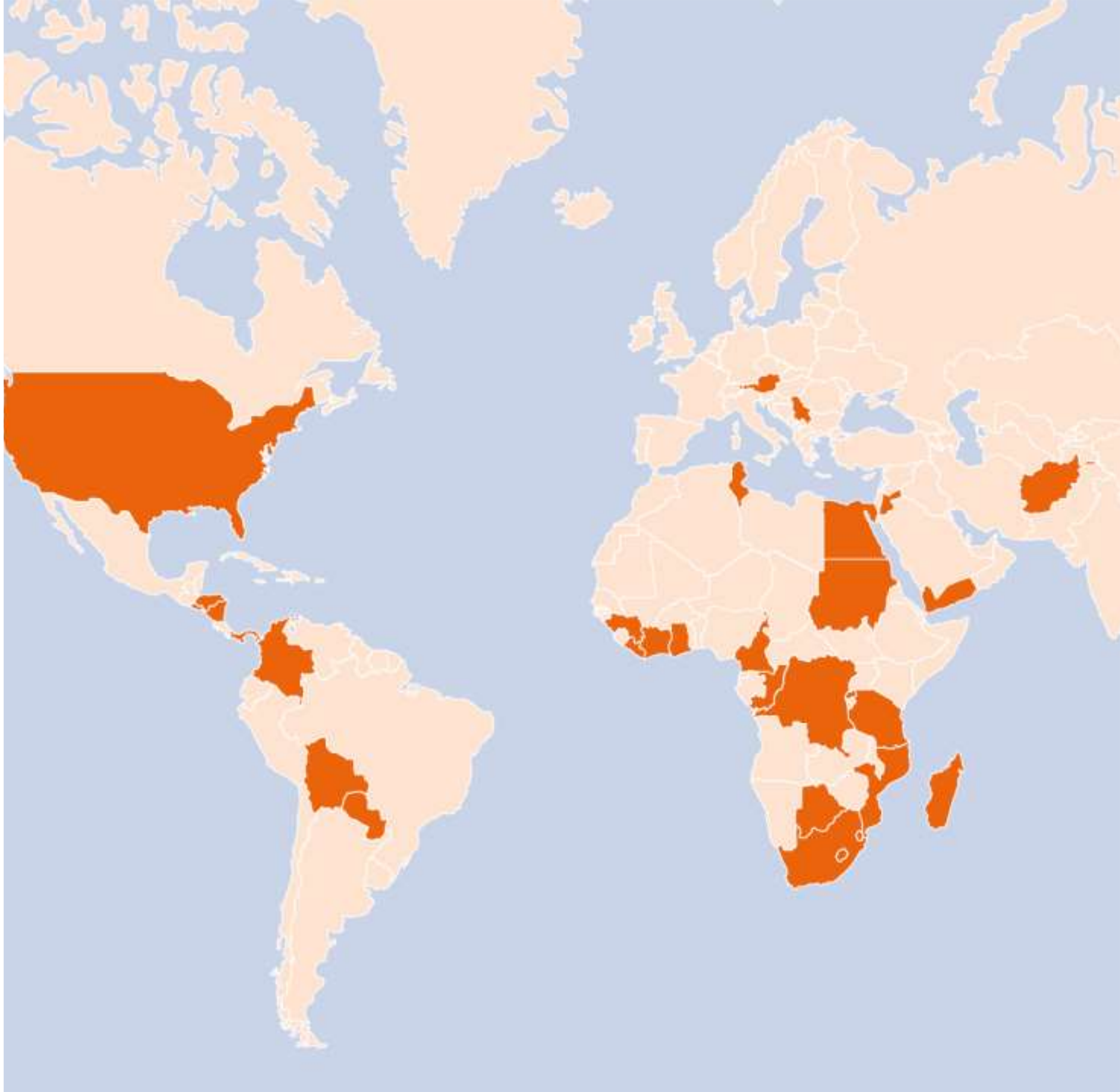
However, research by the GSMA Digital Identity programme has revealed that when a digital ID ecosystem has been built properly and supported by the public and private sector, ID verification during customer on-boarding can provide commercial benefits and opportunities for MNOs. It may also help governments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

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.

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.

Full report:
www.gsma.com/mobilefordevelopment/resources/commercially-sustainable-roles-for-mobile-operators-in-digital-id-ecosystems/



Research snapshot

Ecosystem

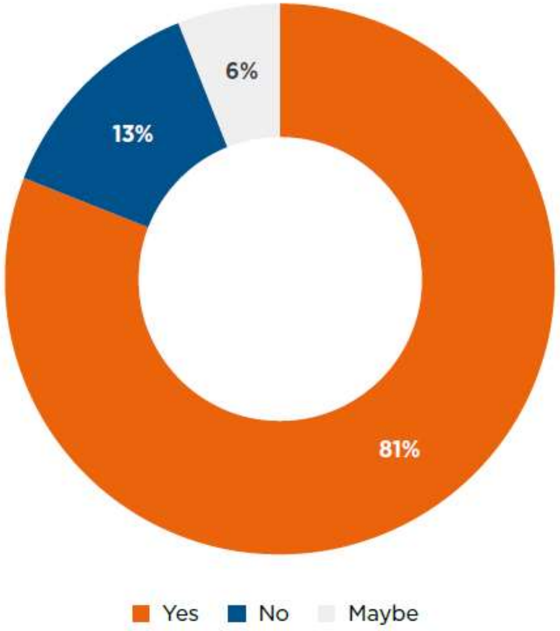
Digital transformation is turning SIM registration from a burden into an opportunity

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.

Ecosystem

81 percent of MNOs consider SIM registration and KYC mandates as a positive opportunity



Top 10 reasons why MNOs consider the mandates a positive opportunity

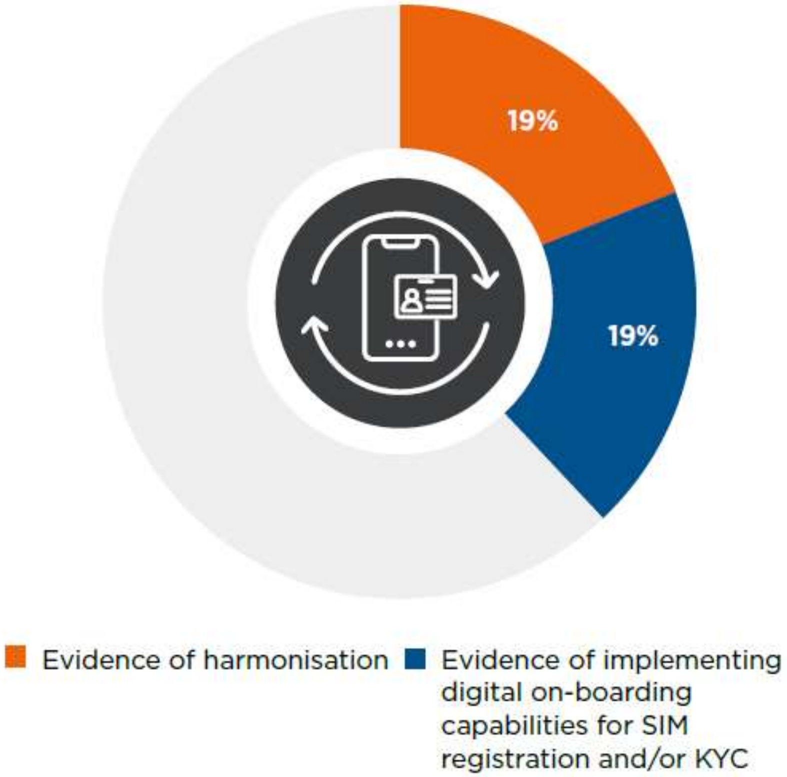
1. Provide new and appropriate products and services
2. Prevention of fraud, AML, cybercrime and other crime
3. Understand customers and spending patterns better
4. Improve national security/supply information
5. Improved customer database
6. Support government
7. Improve customer access to mobile-enabled 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.

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.

Ecosystem

38 percent of MNOs show evidence of harmonisation and new digital implementations



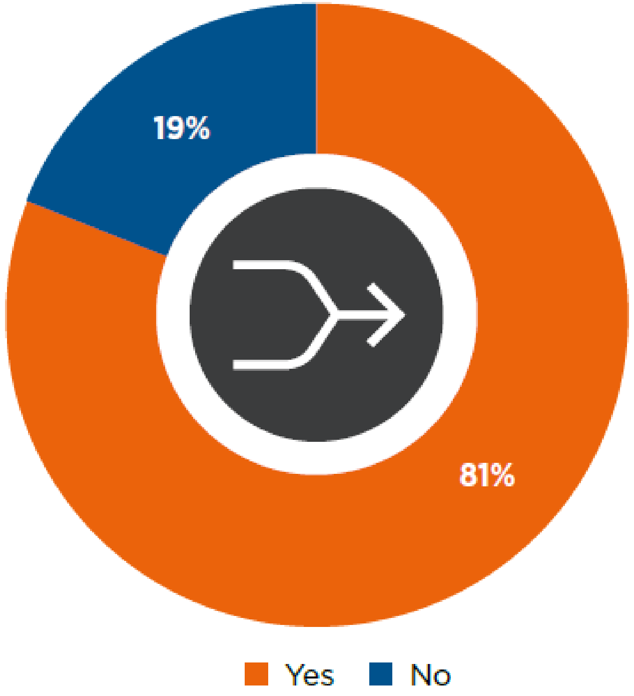
Base: All respondents

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.

However, adoption of digital forms of ID is far from done – of those countries allowing the use of digital ID in SIM-registration and KYC, **over 25 per cent** of customers still use non-digital forms of ID.

Ecosystem

81 percent of MNOs are willing to harmonise SIM registration with mobile money KYC



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?

Over

25%

of customers, in countries allowing the use of digital ID for SIM registration and KYC...

...still use non-digital forms of ID

Research snapshot

Benefits

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

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.

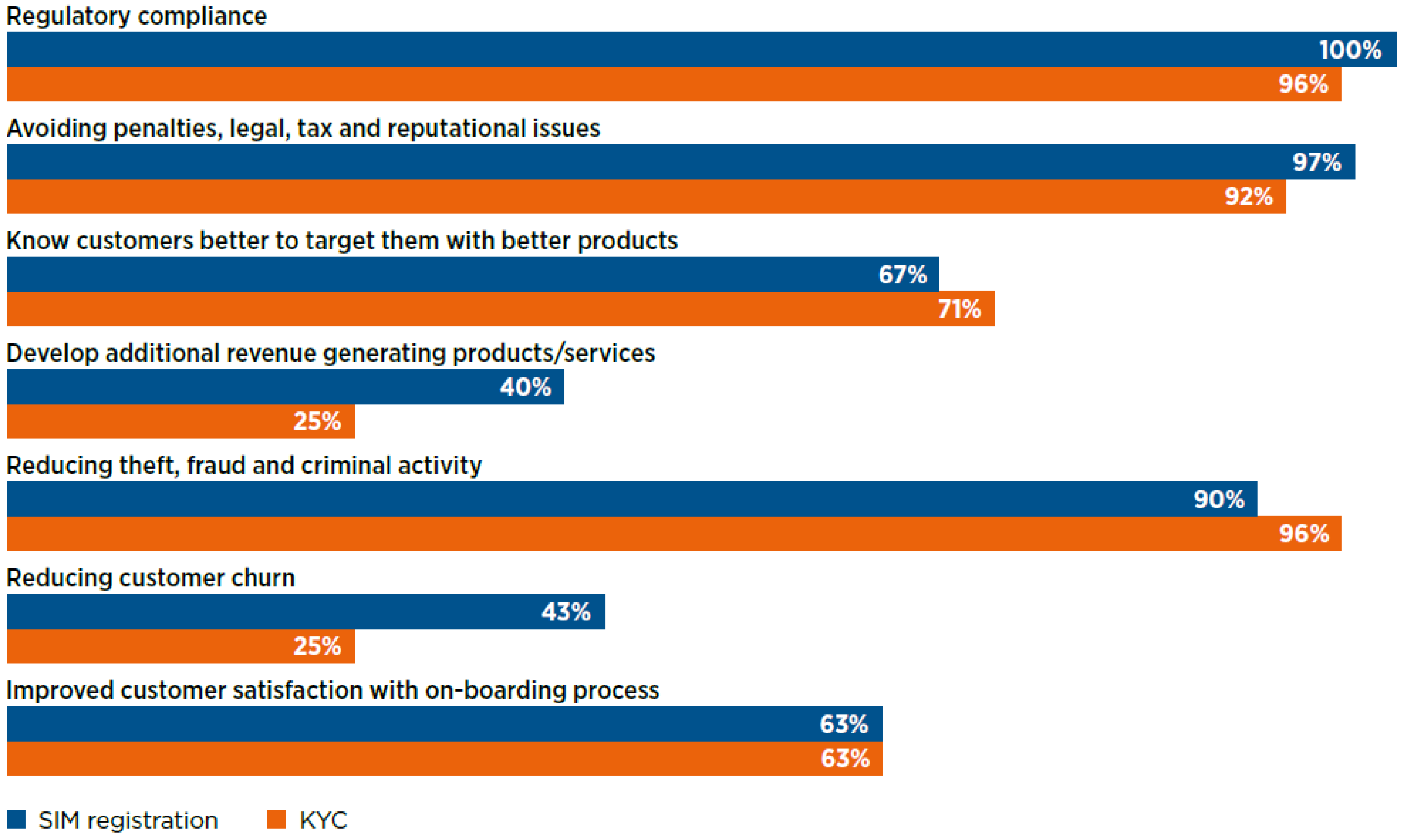
Digitally sophisticated MNOs are **more likely** to cite commercial benefits as the main advantages of their investment in their ecosystem with some having already **generated revenue** from ID-linked mobile services.

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.

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.

Benefits

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

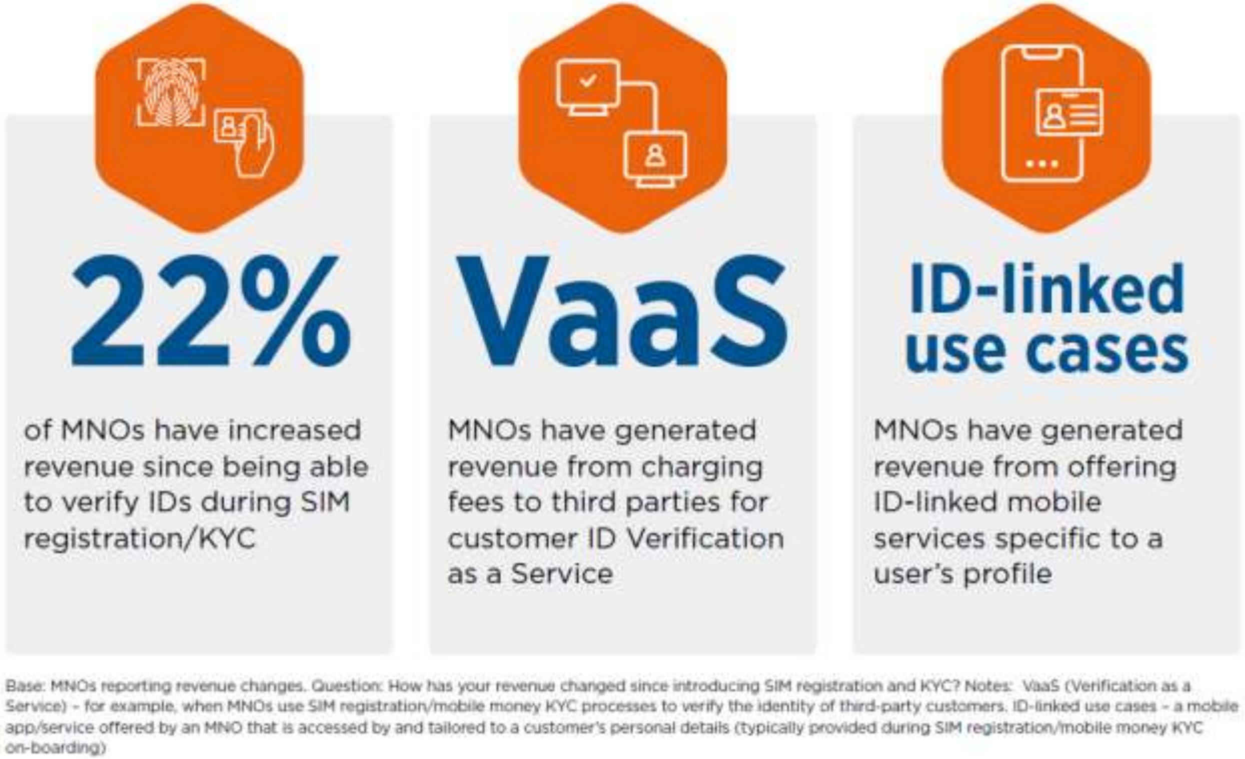


Base: All respondents. Question: What are the main benefits of your investment in SIM registration and KYC?

Several MNOs report that they have already increased revenue through such services.

Benefits

MNOs have benefited commercially from leveraging SIM registration and KYC



22%

of MNOs have increased revenue since being able to verify IDs during SIM registration/KYC

VaaS

MNOs have generated revenue from charging fees to third parties for customer ID Verification as a Service

ID-linked use cases

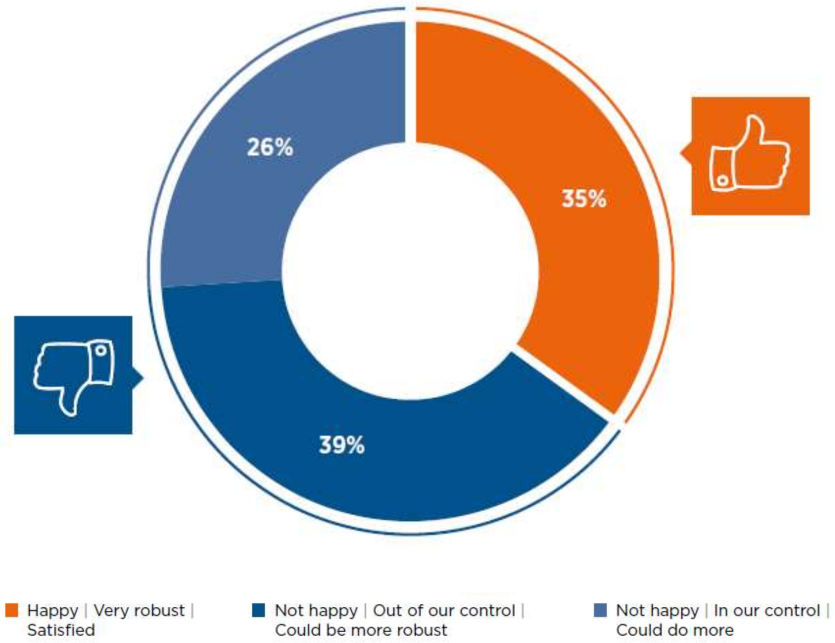
MNOs have generated revenue from offering ID-linked mobile services specific to a user's profile

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)

A third of MNOs are happy and satisfied with the robustness of their ecosystem, providing an aspirational benchmark for the industry.

Benefits

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?

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.

Research snapshot

Opportunities

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

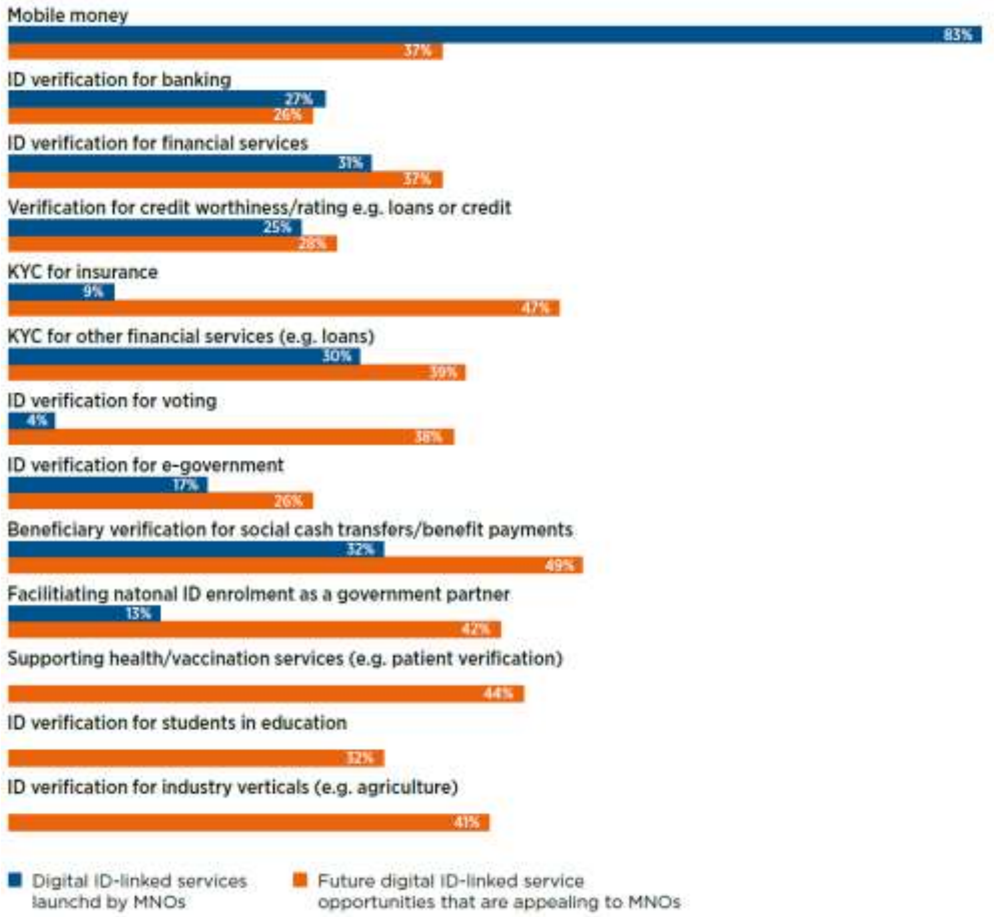
Offering ID-linked mobile financial services (aside from mobile money) currently appears to be the greatest revenue-earning opportunity for MNOs keen to invest in digital ID verification.

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.

Opportunities

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

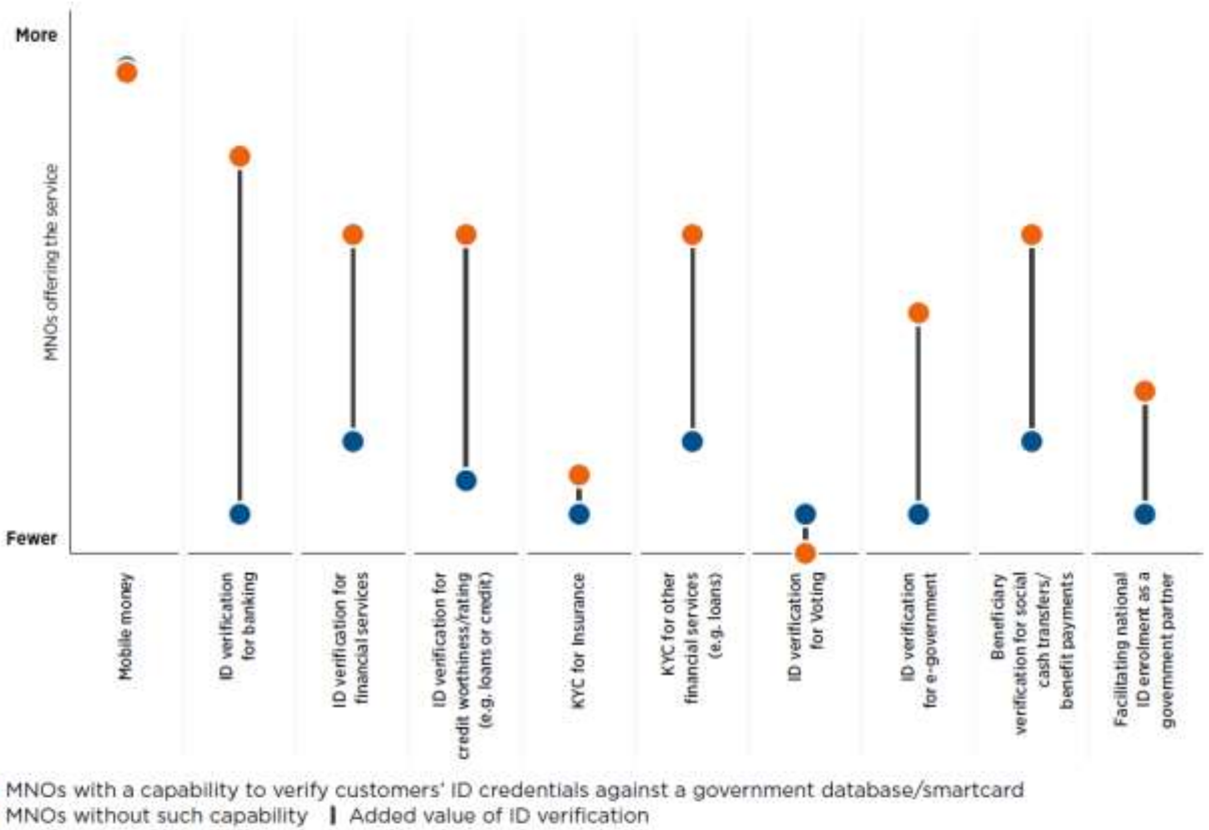


Base: All respondents. Question: Have you targeted customers with personalised mobile services after introducing a SIM registration process and, looking to the future, which mobile services do you find appealing to offer your identified customers? Note: While MNOs in this sample have said they do not 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.

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.

Opportunities

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



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

Opportunities

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).

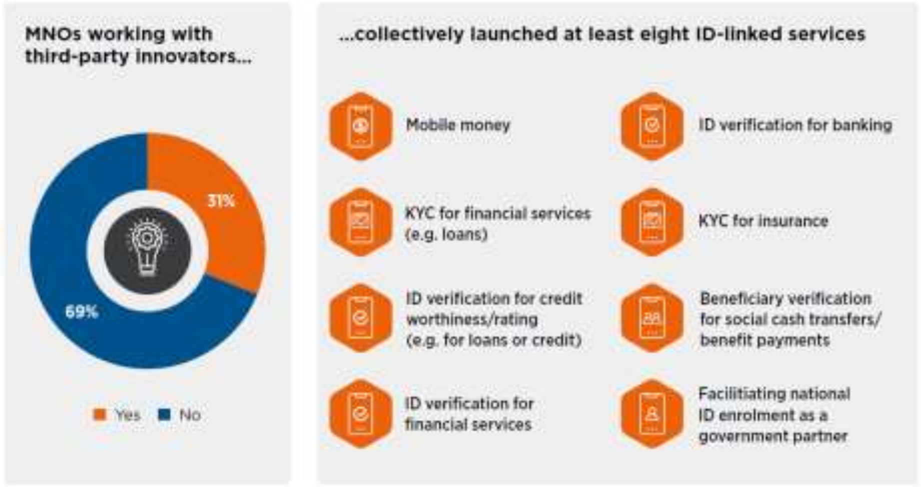
MNOs have a strong appetite for partnerships with innovators in the digital identity space.

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.

MNOs with digitised ID verification processes are **more likely** to have worked with innovators.

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



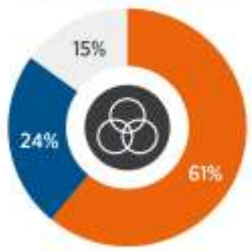
...collectively launched at least eight ID-linked services

- Mobile money
- ID verification for banking
- KYC for financial services (e.g. loans)
- KYC for insurance
- ID verification for credit worthiness/rating (e.g. for loans or credit)
- Beneficiary verification for social cash transfers/ benefit payments
- ID verification for financial services
- Facilitating national ID enrolment as a government partner

Various MNOs have also launched services on their own.

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?

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



Base: All respondents. Question: In future, would you be willing to work with third-party innovators on new services?

Research snapshot

Costs

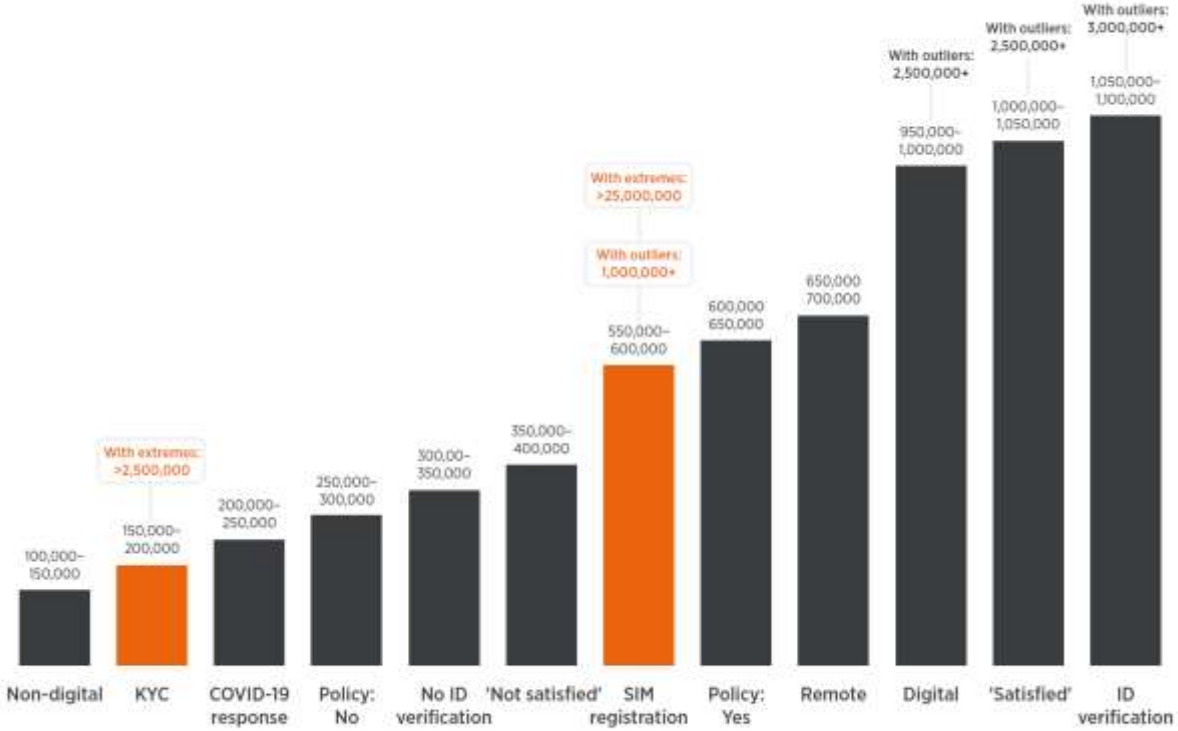
Digital ID verification costs more but many MNOs predict it will pay off

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.

Costs

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

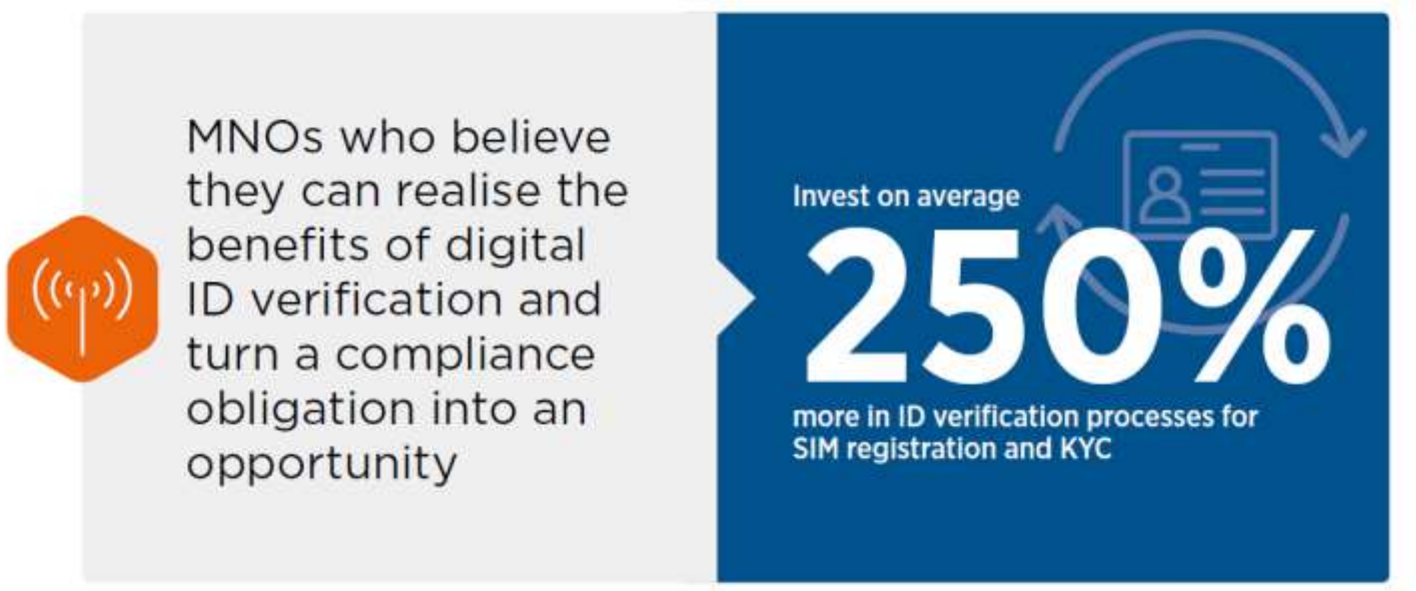


Base: All respondents. Question: What was your overall cost for setting up SIM registration and mobile money KYC processes? Notes: Figure 27 shows average overall set-up cost (in USD) of an MNO's SIM registration and mobile money KYC processes. Costs in some instances are converted from local currency 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).

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.

Costs

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



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

Invest on average

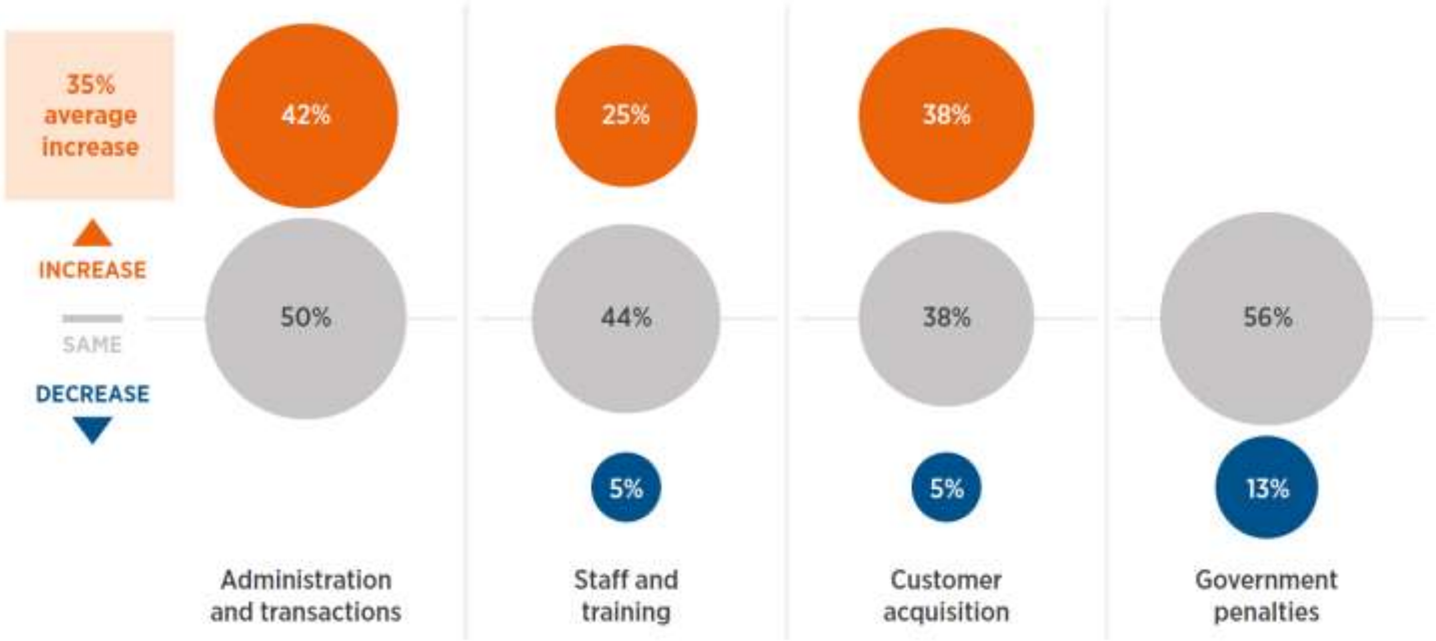
250%

more in ID verification processes for SIM registration and KYC

Some MNOs say that, on average, since roll-out of their SIM registration processes, costs have **increased up to 35 per cent** with some citing administration, customer acquisition and staff costs increases.

Costs

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

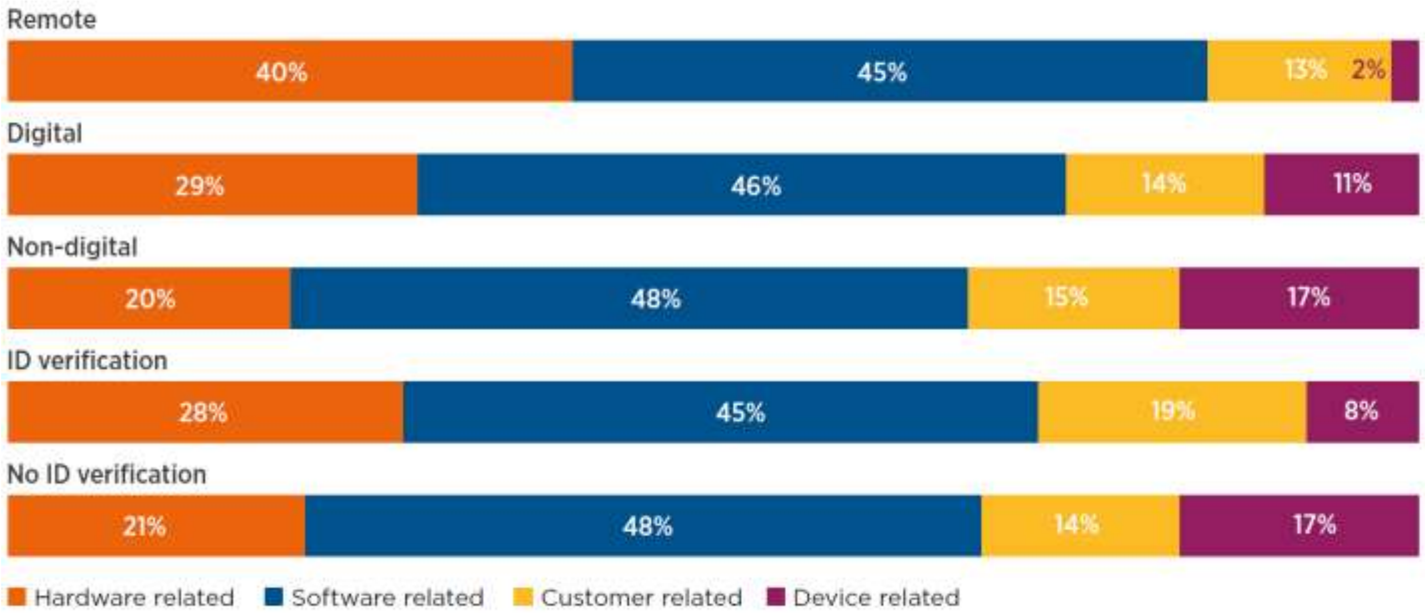


Base: MNOs reporting cost base fluctuations since implementing SIM registration processes. Question: How have your costs changed since introducing SIM registration and KYC? Note: Bubbles represent the percentage of MNOs reporting cost base fluctuations since introducing SIM registration processes

The proportion of CAPEX spent on hardware **(e.g. servers, network equipment)** for MNOs with remote ID-verification is **double that** of those with in-person only (non-digital) ID-verification.

Costs

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



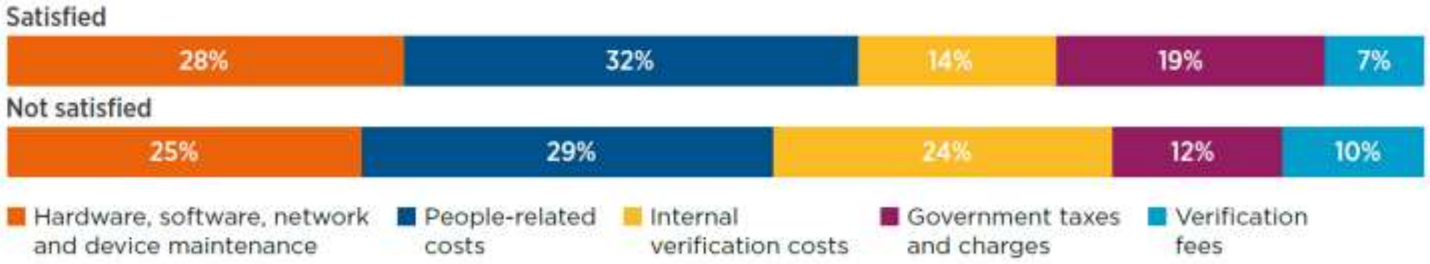
Base: All respondents. Question: What was your estimated CAPEX to set up your SIM registration and KYC processes? Notes: **Remote -** MNOs with ID verification capabilities, such as the ability to on-board oneself via a mobile phone. **Digital -** MNOs with all digital forms of ID verification. **Non-digital -** 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)

Costs

MNOs satisfied with their ecosystem implementations **invest more in people**, however, people related operational costs decrease with ecosystem digital sophistication.

MNOs satisfied with their ecosystem robustness **spend less on internal verification** costs. Although 18 per cent do so for free, around **15 per cent of MNOs** spend externally on ID verification and query a government database/smartcard. Many more MNOs are **interested** in adopting this.

OPEX: 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

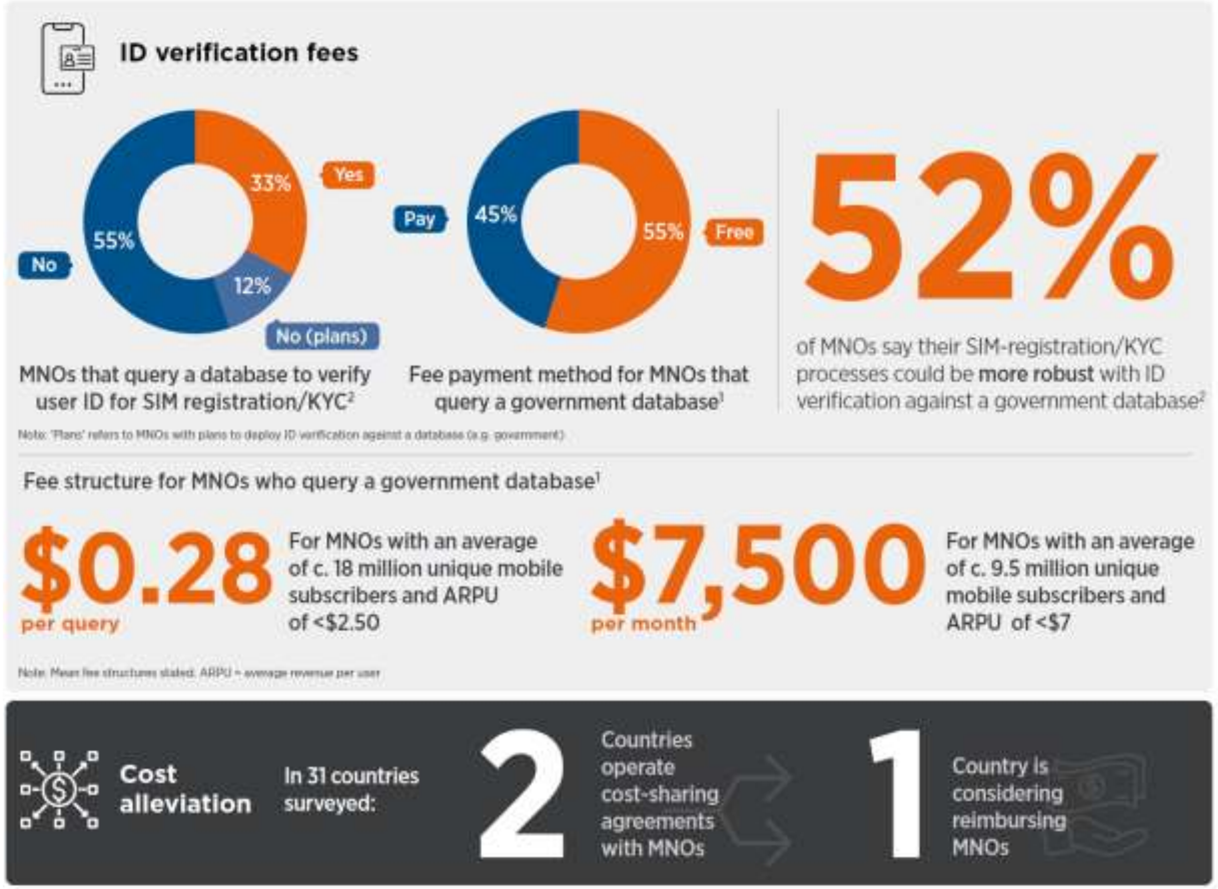
Of the MNOs capable of verifying IDs against a government database, **45 per cent** pay ID verification fees for each query (averaging $0.28), although some report that they pay a monthly fee (averaging $7,500 a month) instead.

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.

Costs

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



ID verification fees

MNOs that query a database to verify user ID for SIM registration/KYC[2]

Fee payment method for MNOs that query a government database[1]

52% of MNOs say their SIM-registration/KYC processes could be **more robust** with ID verification against a government database[2]

Note: 'Plans' refers to MNOs with plans to deploy ID verification against a database (e.g. government)

Fee structure for MNOs who query a government database[1]

$0.28 per query — For MNOs with an average of c. 18 million unique mobile subscribers and ARPU of <$2.50

$7,500 per month — For MNOs with an average of c. 9.5 million unique mobile subscribers and ARPU of <$7

Note: Mean fee structures stated. ARPU = average revenue per user

Cost alleviation — In 31 countries surveyed:

2 Countries operate cost-sharing agreements with MNOs

1 Country is considering reimbursing MNOs

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?

Research snapshot

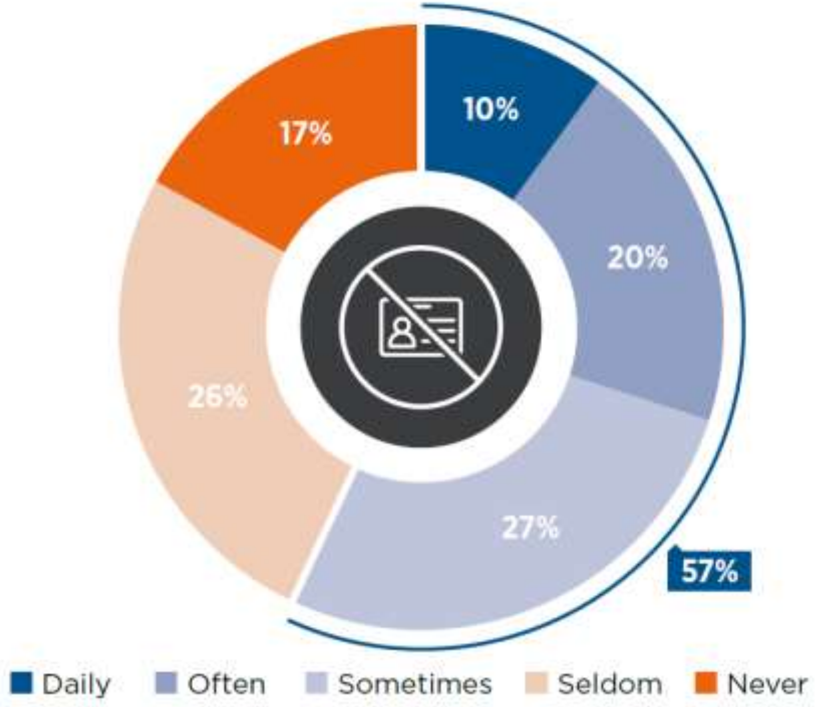
Threats

Robust customer ID verification is still a challenge for many MNOs

57 per cent of MNOs are often unable to on-board customers because they lack the requisite identity credentials.

Threats

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



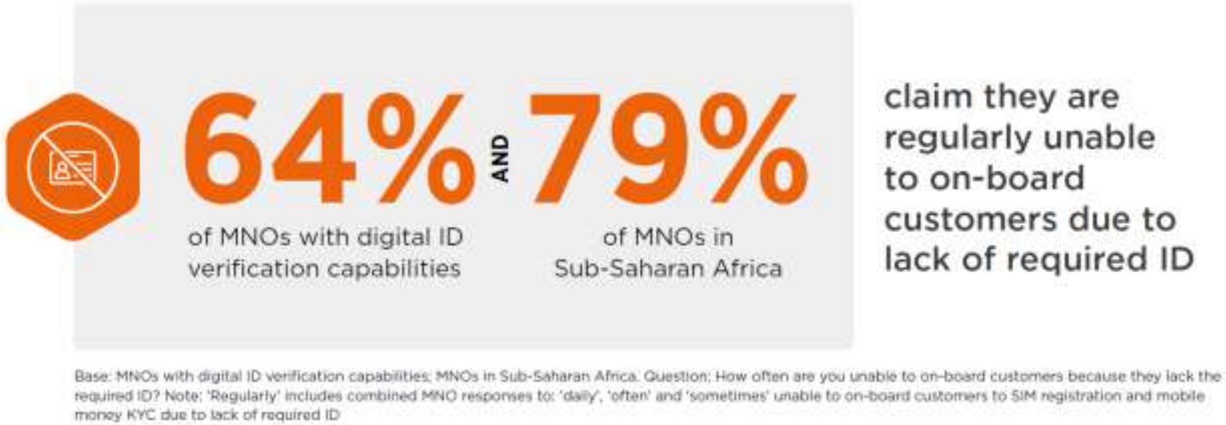
Base: All respondents. Question: How often are you unable to on-board customers because they lack the required ID?

MNOs with digital ID verification capabilities, in general, are more often unable to on-board customers. This is also the case among MNOs in the Sub-Saharan Africa region.

However, MNOs with more digitally sophisticated ID verification capabilities such as remote on-boarding and ID verification against a government database or smartcard token, tend to experience fewer on-boarding issues because customers lack the requisite identity credentials.

Threats

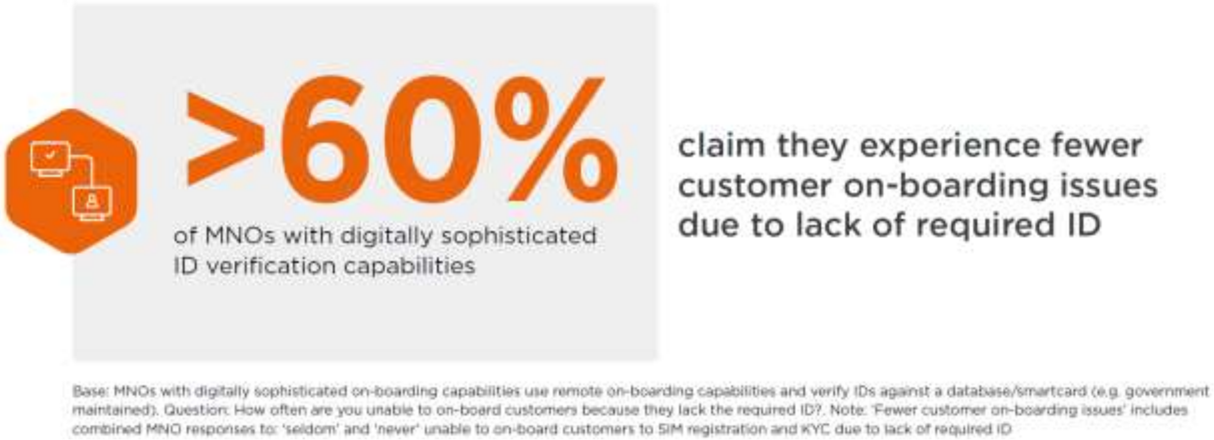
MNOs in some contexts experience more customer on-boarding issues



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 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

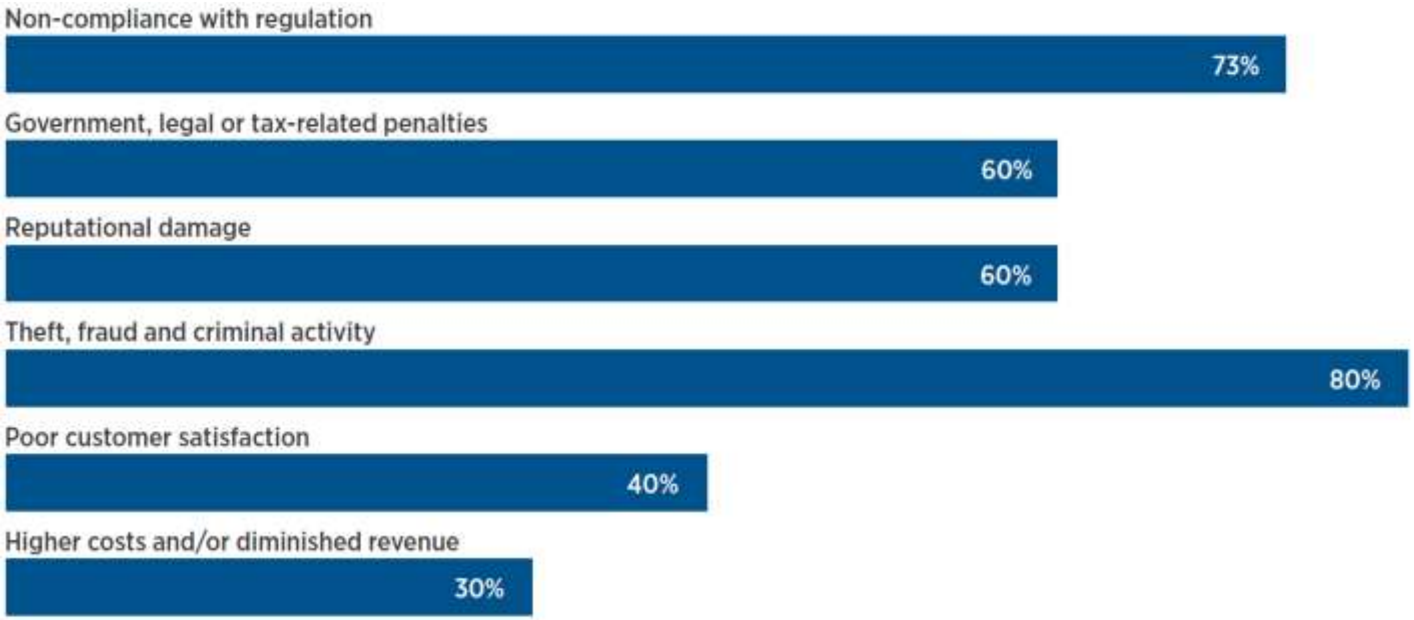
Threats

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.

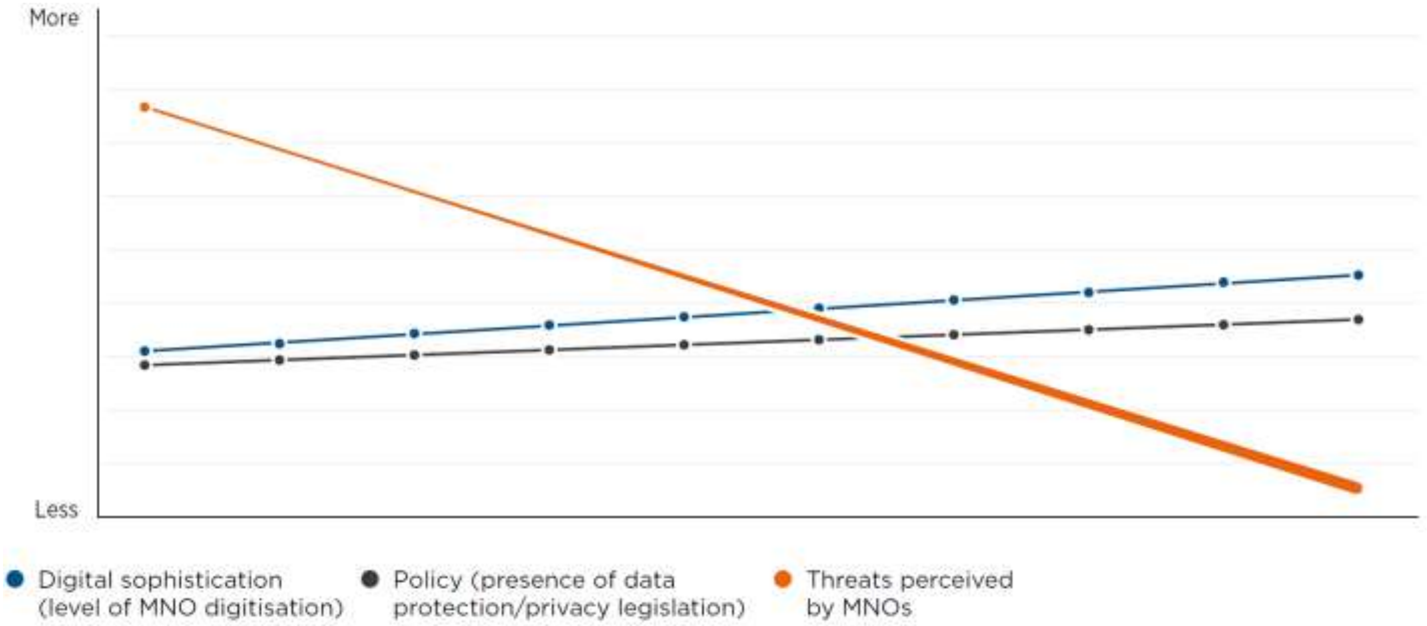
The main threats to MNOs when validating IDs for SIM registration and mobile money KYC processes are criminal activity and regulatory non-compliance



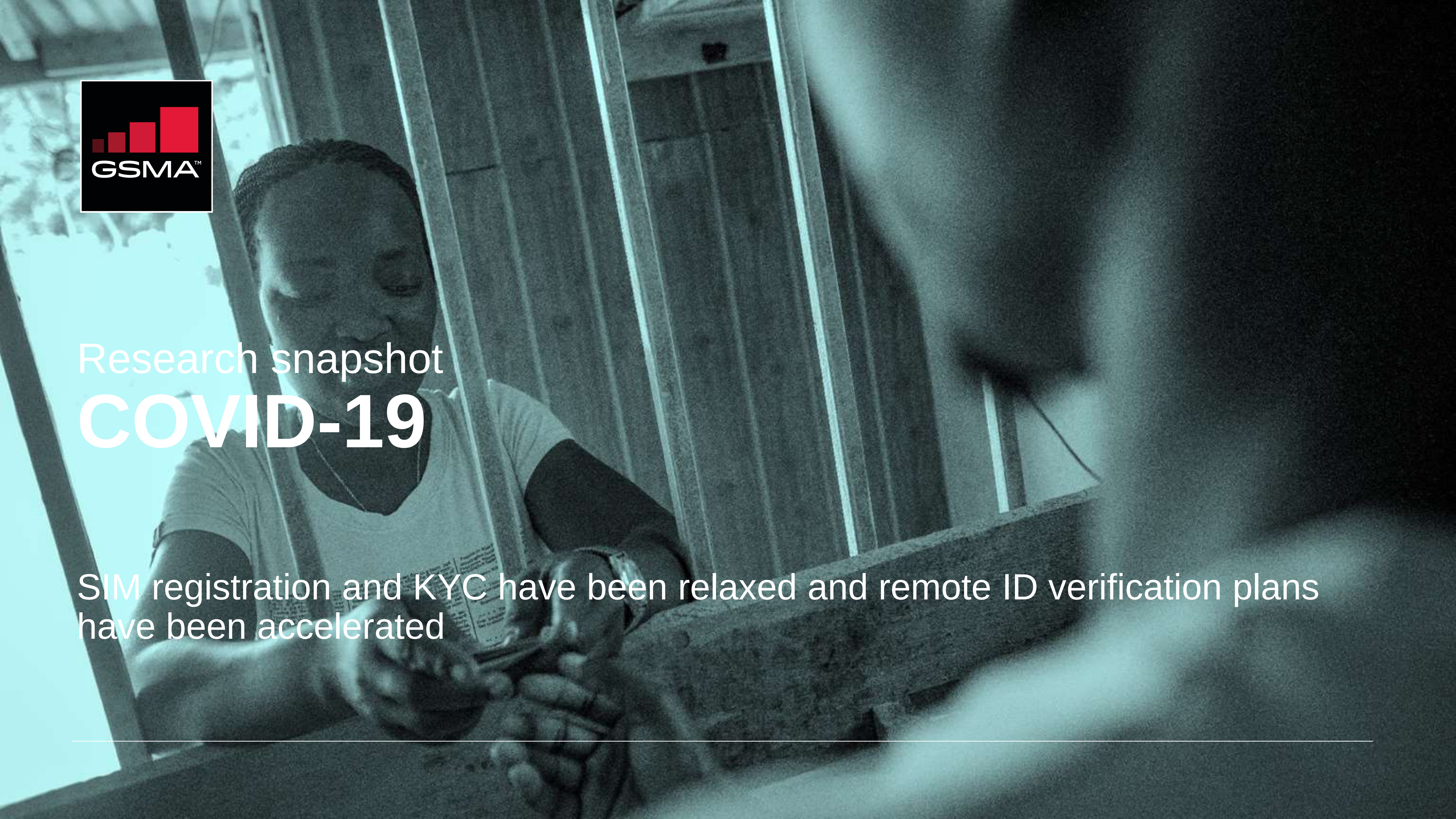
Base: All respondents. Question: What threats do you perceive when validating IDs for SIM registration or KYC purposes?

Threats

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



Research snapshot

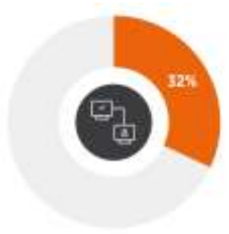
COVID-19

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

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, but also accelerated the digital transformation plans of some MNOs.

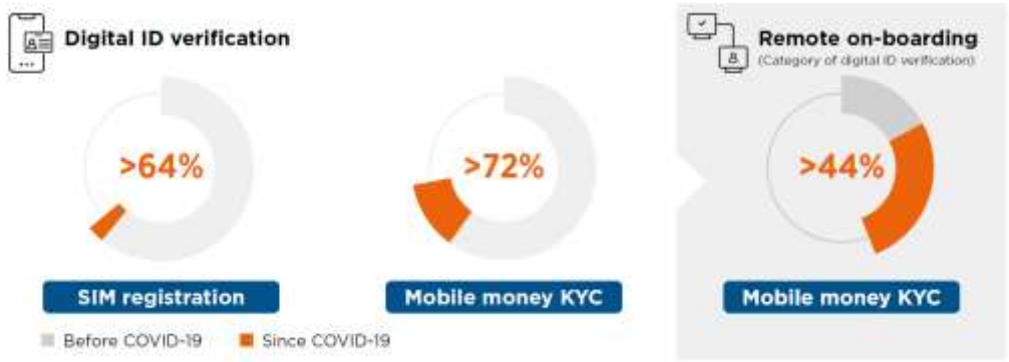
COVID-19

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



Base: All respondents. Question: In response to COVID-19, have you relaxed on-boarding / verification criteria for SIM registration and KYC?

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?

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);

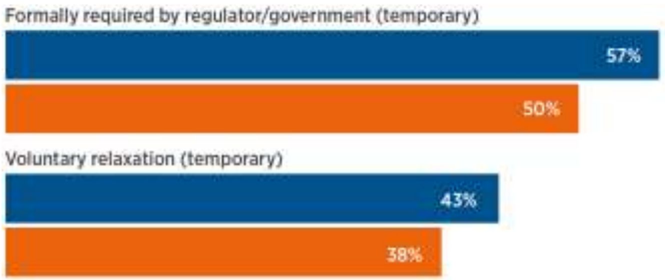
Up to **63 per cent** relaxed ID registration terms (e.g. accepted a wider range of IDs);

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).

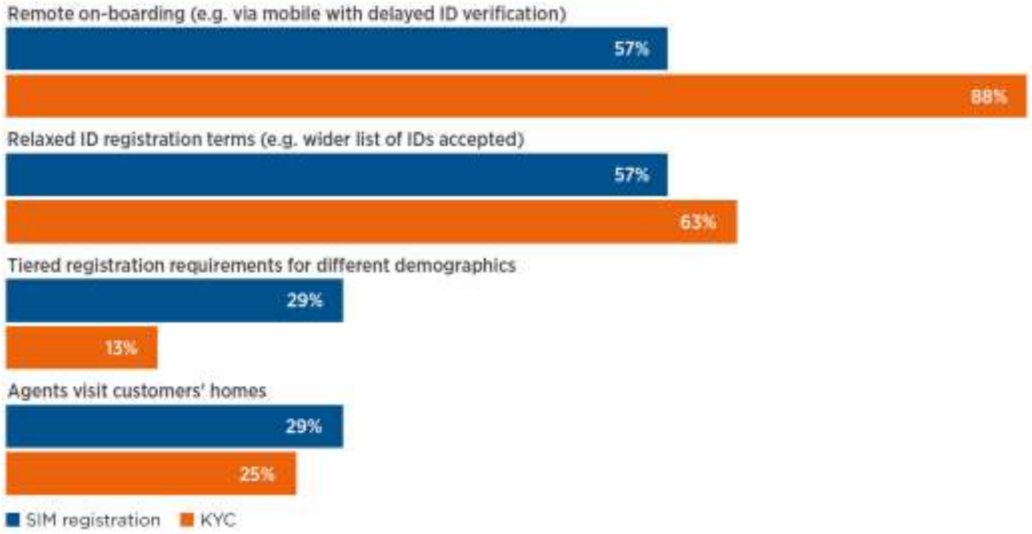
COVID-19

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?

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

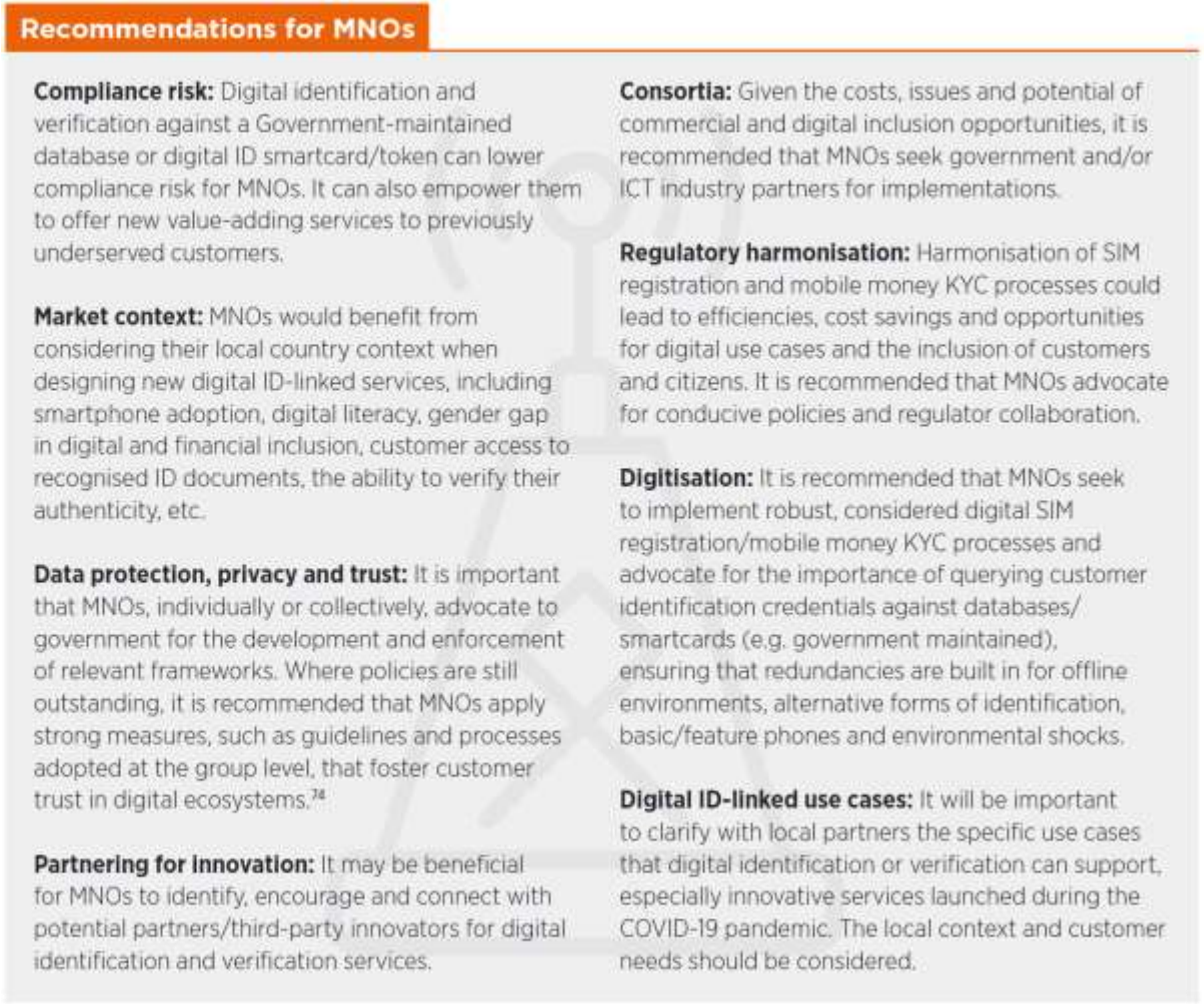


Base: MNOs that responded to COVID-19 by relaxing on-boarding/ID verification requirements. Question: What are the relaxed measures?

Recommendations

Recommendations

The insights from this research, combined with the GSMA Digital Identity programme's experience leading several related initiatives, 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.

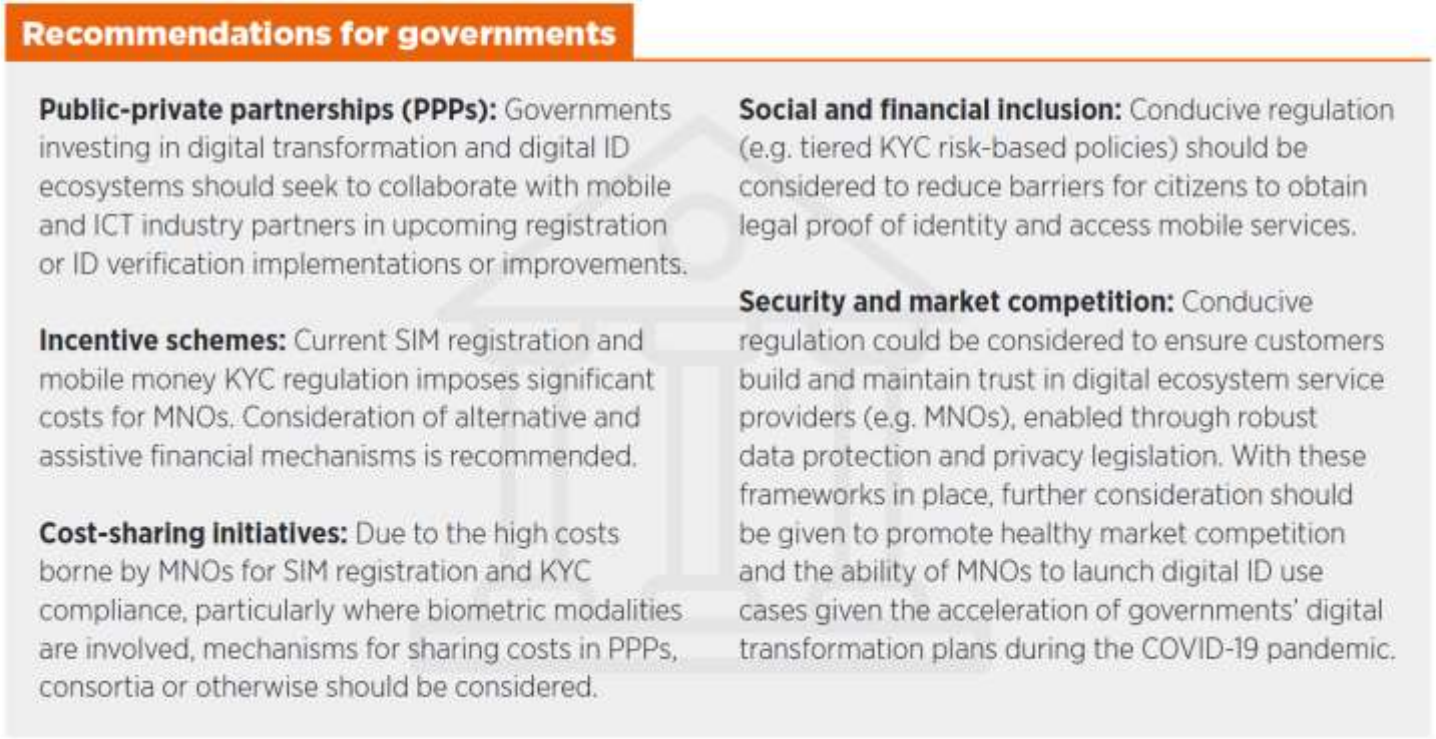
Consortia: Given the costs, issues and potential of commercial and digital inclusion opportunities, it is recommended that MNOs seek government and/or ICT industry partners for implementations.

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.

Recommendations



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. 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.

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. Where required, the Digital Identity team followed up with respondents to explore topics in more detail or to clarify answers.

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.

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

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.

Digital Identity

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

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

Follow GSMA Mobile for Development on Twitter: @GSMAm4d

Authors:

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