Access to Mobile Services and Proof of Identity 2021

Revisiting SIM Registration and Know Your Customer (KYC) Contexts during COVID-19

April 2021

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

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

GSMA Intelligence

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide — from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily. GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision-making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself. Our team of analysts and experts produce regular thought leading research reports across a range of industry topics.

www.gsmaintelligence.com
info@gsmaintelligence.com

At Ipsos we are passionately curious about people, markets, brands and society. We deliver information and analysis that makes our complex world easier and faster to navigate and inspires our clients to make smarter decisions.

With a strong presence in 88 countries, Ipsos employs more than 16,000 people and has the ability to conduct research programmes in more than 100 countries. Founded in France in 1975, Ipsos is controlled and managed by research professionals.

www.ipsos.com

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.

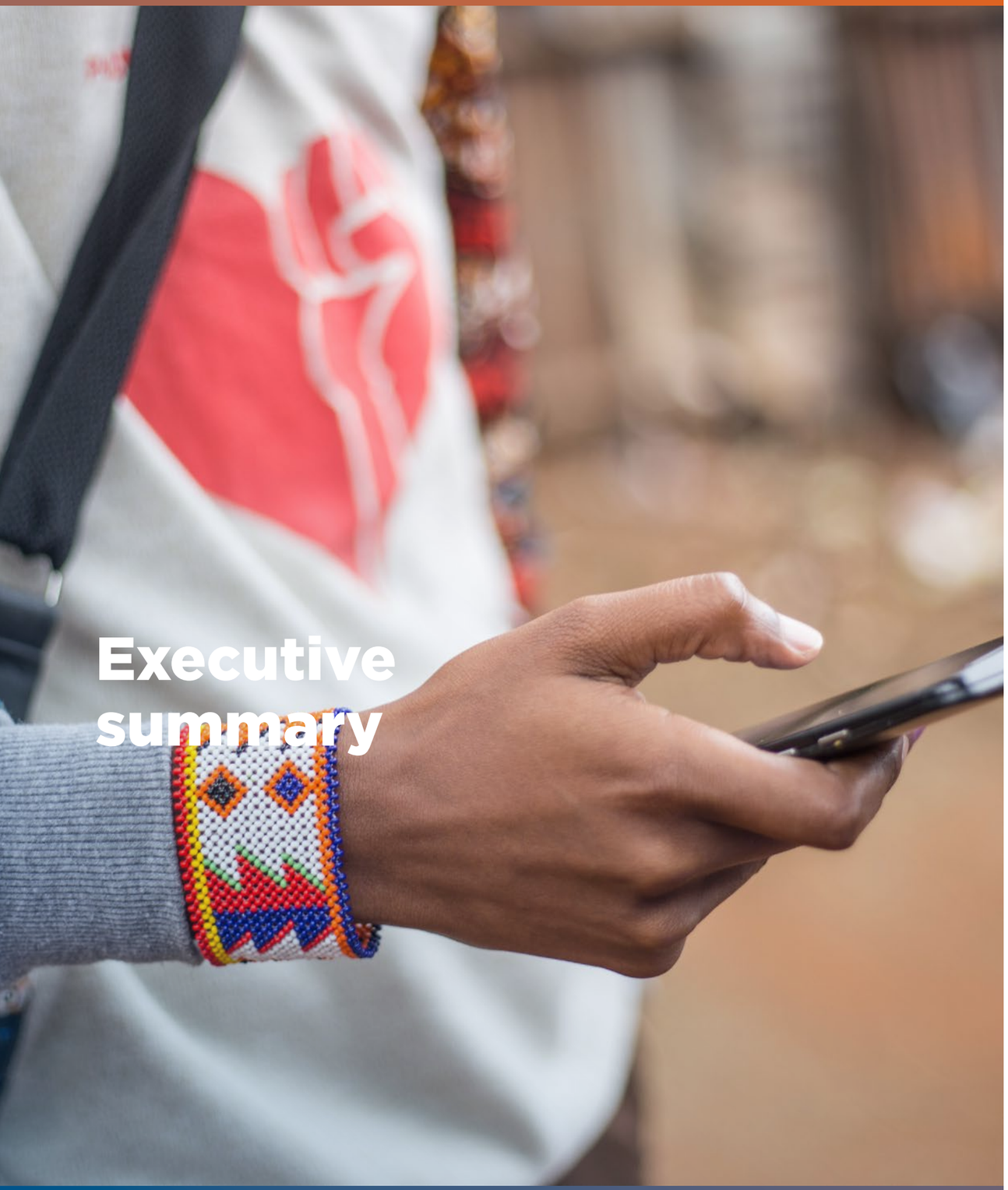
Authors:
Erdoo Yongo, Policy and Advocacy Manager, GSMA
Christopher Lowe, Senior Insights Manager, GSMA
Yiannis Theodorou, Senior Director, GSMA

Contributors:
Cicely Corbin, Operations Manager, GSMA
James Robinson, Lead Analyst, GSMA Intelligence
Kenechi Okeleke, Director, GSMA Intelligence
Caroline Butler, Economist, GSMA Intelligence
Kalvin Bahia, Principal Economist, GSMA Intelligence

Fieldwork partner:
Ipsos worked with the GSMA as a fieldwork partner on one study in this report, the GSMA Consumer Survey 2020. As such, it is not responsible for the analysis or conclusions in this report.

Contents

Executive summary 2
Introduction 8
Mobile connectivity continues to grow globally 10
Accessing mobile services in one's own name remains a challenge 14
Many governments relaxed regulations during the COVID-19 pandemic to facilitate digital and financial inclusion 24
Regulatory relaxations offer opportunities for underserved groups to access mobile services in their own name 34
Building trust in digital ecosystems remains a priority 44
Conclusion and policy recommendations 46
Appendices 50



Executive summary

ACCESS TO MOBILE SERVICES AND PROOF OF IDENTITY 2021

Mobile connectivity continues to grow globally

In 2020, the number of unique mobile subscribers rose to over 5.2 billion worldwide. Prepaid mobile connections fell to 72 per cent over the same period, and while this is a marginal decrease from 2019, prepaid SIM cards remain the predominant modality for connecting to a mobile network globally.[1] When the COVID-19 pandemic took hold in 2020 and restrictions on movement and social distancing became a part of daily life around the world, the importance of mobile for communicating with loved ones and accessing life-enhancing services remotely came into sharp focus.

Yet, for the one billion people globally who do not have the means to prove their identity, accessing SIM cards and mobile services in one's own name remains a challenge, particularly in the 157 countries where SIM registration requirements are mandatory.

The number of countries where mandatory pre-paid SIM registration policies are in place has increased from 155 to 157 in the last year. While this is a modest increase, many governments continue to perceive this policy as an important way to address national security concerns. This is despite the lack of published empirical evidence showing a direct link between the introduction of such policies and a reduction in crime-related activities.[2]

Lack of ID can lead to digital, social and financial exclusion

The GSMA has conducted nationally representative research in seven low- and middle-income countries (LMICs) with a combined population of around 2.1 billion. Where SIM registration is mandatory, 14 per cent of respondents do not have a national ID card and three per cent lack any form of identification.

The overwhelming majority of these individuals are therefore at a higher risk of digital, social and financial exclusion as mobile may be their only means of accessing online information and financial services and receiving social benefits.

Accessing mobile services in one's own name depends heavily on access to official ID

According to this research, 18 per cent of SIM card users[3] do not have a SIM card registered in their own name. If extrapolated across the seven countries, this is estimated to be about 285 million people. Those with an official form of identity are more than twice as likely to have a SIM card registered in their own name (82 per cent) than those without an official form of identity (36 per cent).

1 Based on GSMA Intelligence data on unique mobile subscribers (2020) and prepaid connections (2019 and 2020).

2 GSMA. (2013). The Mandatory Registration of Prepaid SIM Card Users: A White Paper; and GSMA. (2016). Mandatory Registration of Prepaid SIM Cards: Addressing Challenges through Best Practice.

3 SIM card users are defined as those that have a SIM card (i.e. mobile phone number) that they use at least once a month, in a handset that they have sole or main use of or in other people's handsets.

Many governments relaxed proof-of-identity rules during the COVID-19 pandemic to minimise the risk of digital and financial exclusion. This was in recognition of the challenges underserved groups faced in accessing mobile financial services and receiving social benefits.

The spread of COVID-19 in 2020 drastically altered how individuals and businesses could operate. When faced with the question of how to curb the spread of the virus and limit the need for physical interactions, connectivity provided the solutions to enable people to continue working, learning and socialising. To encourage greater access and use of mobile financial services, 37 governments around the world introduced and/or relaxed 93 regulatory measures.[4] One of these measures – flexible KYC and proof-of-identity on-boarding requirements – was researched by the GSMA Digital Identity programme in five countries.

Women are among those most at risk of digital and financial exclusion due to a lack of ID.

The regulatory relaxations introduced in response to the pandemic helped lower the bar for underserved groups to access mobile services in their own name. In the seven LMICs where the GSMA conducted consumer research, the following groups were identified as most at risk of exclusion:

- **Women:** Female SIM card users are 18 per cent less likely to have a SIM card registered in their own name compared with men.
- SIM card users **with disabilities** are 17 per cent less likely to have a SIM card registered in their own name compared with persons without disabilities.
- **Unemployed** SIM card users are 18 per cent less likely to have a SIM card registered in their own name compared with those who are employed.
- SIM card users with **primary education only** are five per cent less likely to have a SIM card registered in their own name than those with secondary education and nine per cent less likely than those with a degree or postgraduate education.
- **Displaced populations described by the UN Refugee Agency (UNHCR) as "persons of concern"** remain at great risk of being digitally and financially excluded, particularly since this population has increased by 16 per cent over the last year.[5] On this basis, there are more people than ever who need humanitarian assistance, but may be unable to obtain it directly because they are unlikely to have the necessary identification credentials (required by their host country) to meet proof-of-identity requirements to access mobile and digital financial services in their own name.

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

5 Based on GSMA analysis of UNHCR's Global Trends 2018 and 2019 datasets.

ACCESS TO MOBILE SERVICES AND PROOF OF IDENTITY 2021

Building trust in digital ecosystems remains a priority as many countries mandating SIM registration still lack comprehensive data protection and privacy frameworks.

A trend identified in previous editions of this report series remains: a significant proportion (37 per cent) of countries mandating SIM registration still lack data protection and privacy frameworks.[6] This may lead to legitimate consumer concerns over how their personal data is accessed, processed and used by various actors in those countries.

There are a number of policies that governments can draw on to establish inclusive identification and life-enhancing services and enable underserved populations to access them.

However, given the wide and growing reach of mobile technology, mobile network operators (MNOs) also have a crucial role to play, especially as more governments around the world embark on digital transformation strategies. The GSMA recommends that policymakers collaborate with MNOs to create an inclusive digital identity ecosystem, for example, by forging partnerships to support the enrolment of all people who currently lack formal identification.

6 Based on information from Data Guidance, DLA Piper and Privacy Matters.

AS OF EARLY 2021

SIM registration requires proof of identity.

157 countries require mandatory prepaid SIM registration

72% of all mobile SIM cards used globally are prepaid

93% of prepaid SIM cards are in countries where proof of identity is required for mandatory SIM registration

13% of countries with mandatory SIM registration empower mobile operators to validate customers' ID credentials against a government database or token

37% of countries with mandatory SIM registration lack a comprehensive data protection or privacy framework

Proof of identity allows an individual to have a SIM card registered in their own name and, particularly for the underserved, to have access to a plethora of empowering mobile services.

In seven LMICs with a combined population of around **2.1 billion** GSMA Consumer Survey 2020[7]

3% of respondents do not have an official form of ID

14% do not have a national ID card

18% of SIM card users[8] do not have a SIM card registerd in their own name

Certain underserved groups are less likely to have a SIM card registered in their own name

- WOMEN
- UNEMPLOYED
- PERSONS WITH DISABILITIES
- PRIMARY EDUCATED ONLY

Regulatory relaxations during COVID-19 have lowered the identity and on-boarding requirements for SIM registration and mobile money KYC, promoting digital and financial inclusion.

Governments in at least **11 countries** relaxed KYC ID/on-boarding regulatory requirements
GSMA Digital Identity COVID-19 KYC Policy Relaxation Research 2020[9]

Among mobile operators in 31 countries, **32%** relaxed their SIM registration and KYC ID verification/on-boarding requirements
GSMA Digital Identity MNO Survey 2020[10]

Measures often used in response to the regulatory relaxations:

- Remote ID verification/ on-boarding
- Accepting a wider range of IDs
- Harmonisation of SIM registration and mobile money KYC requirements

7 Nationally representative consumer survey of 8000 respondents in Algeria, Bangladesh, India, Kenya, Mozambique, Nigeria and Pakistan

8 SIM card users are defined as those that have a SIM card (i.e. mobile phone number) that they use at least once a month, in a handset that they have sole or main use of or in other people's handsets.

9 Research in Colombia, Ghana, Jordan, Pakistan and Senegal among 31 organisations, see Lowe, C. et al. (2021). **Digital identity: accelerating financial inclusion during a crisis**. GSMA.

10 Research in 31 countries, predominantly in LMICs, among a sample of MNOs. See Lowe, C. and Theodorou, Y. (2021). **Commercially sustainable roles for mobile operators in digital ID ecosystems**. GSMA.

Introduction

The ability to prove one's identity is essential to securing rights and access to life-enhancing services, including healthcare, voting and employment. Identification is also critical to accessing mobile services, especially in countries that have implemented mandatory SIM registration policies. These policies require mobile operators to capture and/or verify their customers' identification credentials and other personal information in order to register or activate a mobile SIM card in their name.

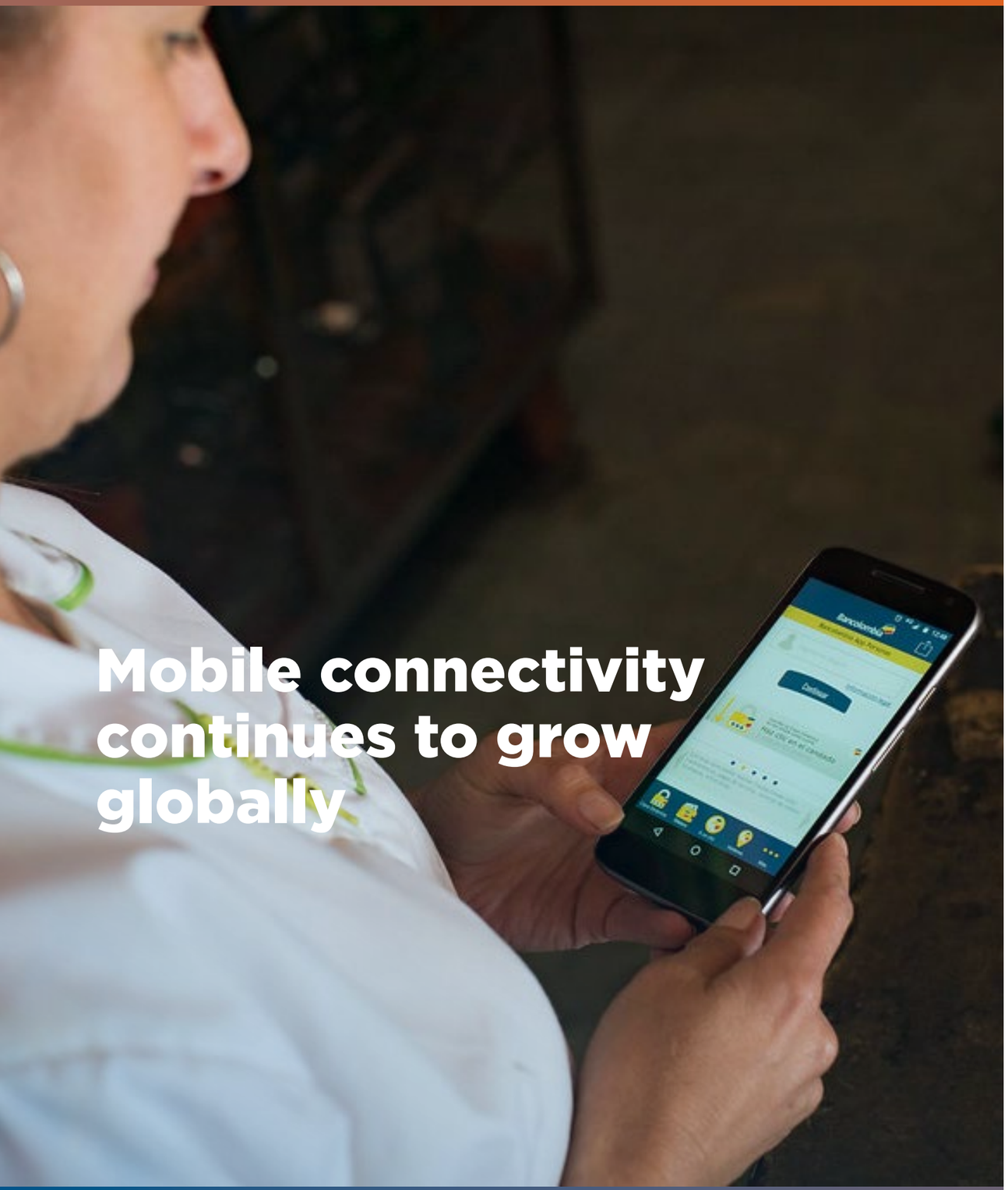
In this 2021 edition of the *Access to Mobile Services and Proof of Identity* series, we provide an update on the countries introducing mandatory SIM registration policies, their various implementation models and whether they have data protection and data privacy frameworks. We also explore trends around access to mobile in one's own name from a consumer perspective, including the impact of the COVID-19 pandemic on underserved groups and the mindset of policymakers.

This year, in addition to referencing existing trusted data sources, the GSMA is able to leverage findings from its own primary and original research to draw out these connections.

The COVID-19 pandemic that disrupted 2020 is the lens through which this report examines changes to identity ecosystems. It is informed by qualitative research conducted with key stakeholders in five countries across the globe, which shone a light on collaborations between the public and private sector to prioritise digital and financial inclusion. Through semi-structured interviews with executives, we highlight the link between access to ID and access to mobile. The result is a comprehensive overview of the regulatory changes and processes implemented in response to the COVID-19 pandemic, and the early impacts on businesses and individuals in Colombia, Ghana, Jordan, Pakistan and Senegal.

For the first time, the annual *Access to Mobile Services and Proof of Identity* report also includes insights from consumer research. We share the highlights of nationally representative quantitative research in seven LMICs that explored consumer perspectives on ID and SIM ownership, and access to ID-linked mobile services in one's own name. This research revealed the extent of the mobile access gap, which is greatest for women, the unemployed and persons with disabilities.

In addition to the GSMA Digital Identity programme's own data and original research, this report captures insights from a range of other sources, including GSMA Intelligence, national telecommunications regulators, the International Telecommunication Union (ITU), the World Bank, various UN agencies, and government, media and civil society reports.



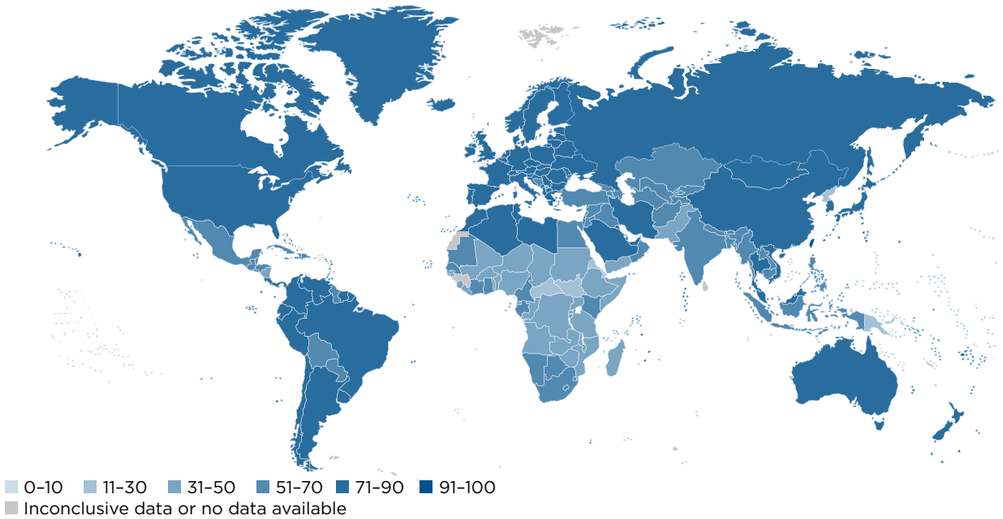
Mobile connectivity continues to grow globally

Although global mobile penetration (i.e. unique mobile subscriptions) remained steady at 67 per cent,[11] 2020 was a year in which mobile connectivity became more important than ever. The COVID-19 pandemic demonstrated just how vital it is for individuals to have access to mobile services. In addition to enabling access to critical health information, digital platforms also supported individuals with remote learning and enabled them to receive social protection payments from their government that, in most cases, safeguarded them from the financial impact of lockdown measures. Connectivity has truly been a lifeline.

As shown in Figure 1 below, mobile coverage is highest in Europe, the Americas and Oceania.[12] Yet, the biggest yearly growth in mobile penetration was in Asia where the number of unique mobile subscribers grew by 6.6 million.[13] Mobile technology is expected to become more important in the future, with unique mobile subscribers set to increase from 5.2 billion (in 2020) to 5.8 billion (by 2025).[14]

Figure 1

Mobile penetration in 2020 (unique subscribers)[15]

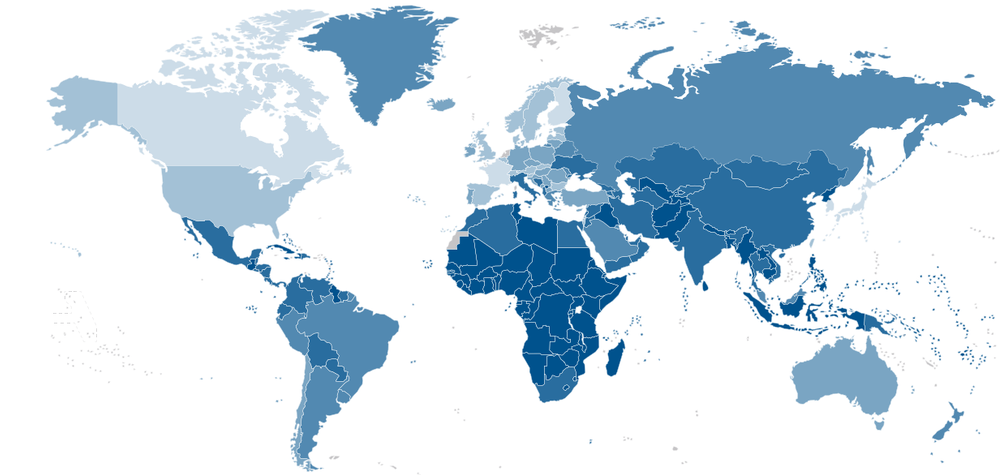


11 GSMA Intelligence, mobile penetration (unique mobile subscribers, Q3, 2020).
12 Ibid.
13 Ibid.
14 GSMA Intelligence (2020), The Mobile Economy 2020.
15 Based on data from GSMA Intelligence, mobile penetration (unique mobile subscribers, Q3, 2020).

Although there was a one per cent yearly decrease in the number of prepaid mobile connections across the world, the majority (72 per cent) of mobile subscriptions remain prepaid as of Q3 2020 (see Figure 2).[16] The average share of prepaid mobile subscriptions (excluding M2M)[17] in Africa is 94 per cent, followed by Asia at 77 per cent, the Americas at 53 per cent, Europe at 47 per cent and Oceania at 42 per cent.[18]

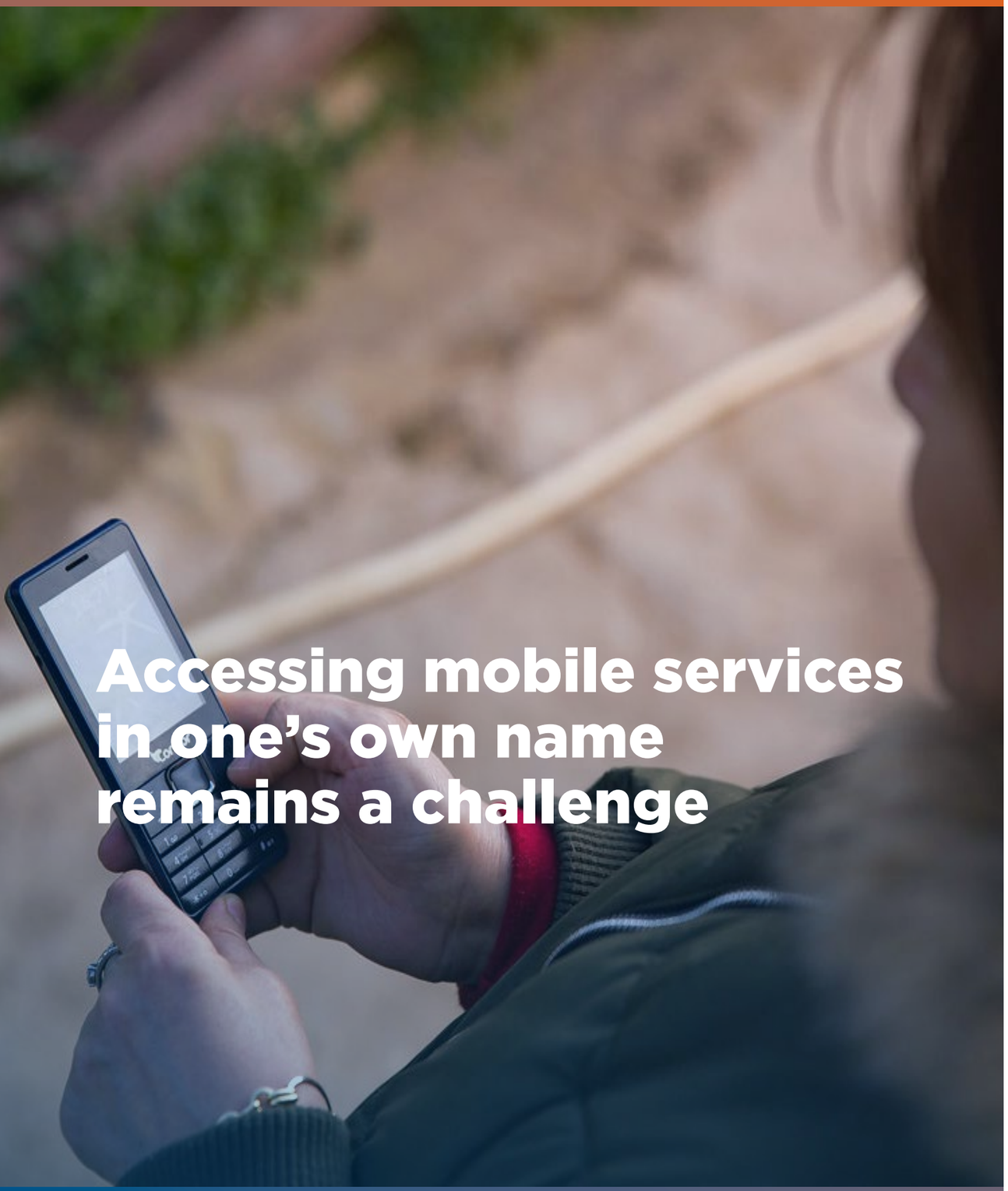
Figure 2

Prepaid SIM penetration[19]



16 GSMA Intelligence, prepaid penetration (prepaid connections, Q3, 2020).
17 M2M = machine to machine
18 Ibid.
19 Ibid.

ACCESS TO MOBILE SERVICES AND PROOF OF IDENTITY 2021



Accessing mobile services in one's own name remains a challenge

ACCESS TO MOBILE SERVICES AND PROOF OF IDENTITY 2021

Prepaid SIM registration is mandatory in 157 countries

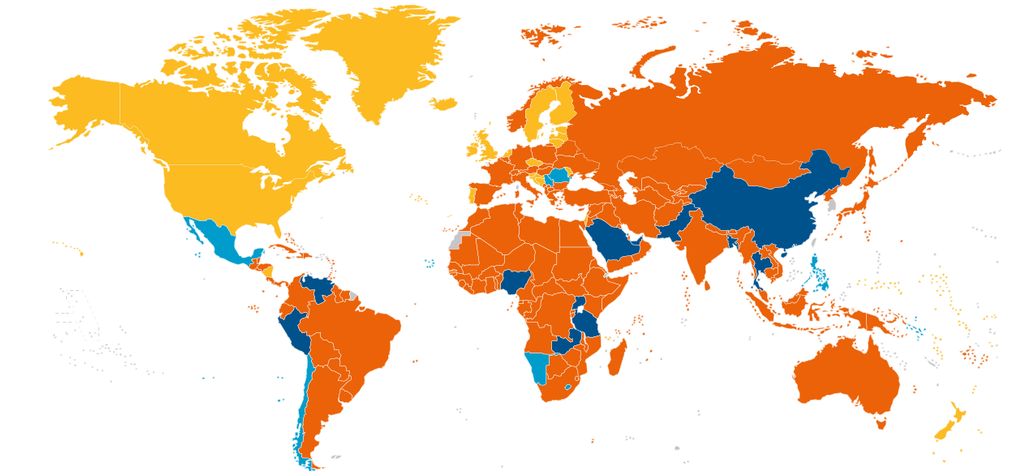
Mandatory SIM registration is a regulatory policy that requires MNOs to capture and/or verify their customers' identification credentials and other personal information (such as name, ID number and address) in order to register or activate a prepaid mobile SIM card in their name. As of February 2021, the GSMA found that governments of 157 countries mandate prepaid SIM registration policies[20] (see Figure 3). Those who do not register their SIM card risk being disconnected from mobile services by their mobile providers.

There was little change in 2020 in the number of countries enforcing biometric SIM registration. Eight per cent of governments mandating this policy require MNOs to collect biometric data from users, such as fingerprints and iris scans, to register them for a prepaid SIM card.

Beyond the 157 countries where this policy is effective, 10 additional countries are considering introducing it. This includes Mexico, a country that had relinquished its SIM registration policy, but is now contemplating reintroducing proof-of-identity requirements for accessing mobile services. This policy would be part of broader amendments to the Federal Telecommunications and Broadcasting Law.[21]

Figure 3

SIM registration status globally[22]



20 See the Appendices for the full list of countries.

21 Mascellino, A. (18 January 2021). "Mexico's national biometric register of mobile phone users proposal advances", BiometricUpdate.com.

22 Based on publicly available information.

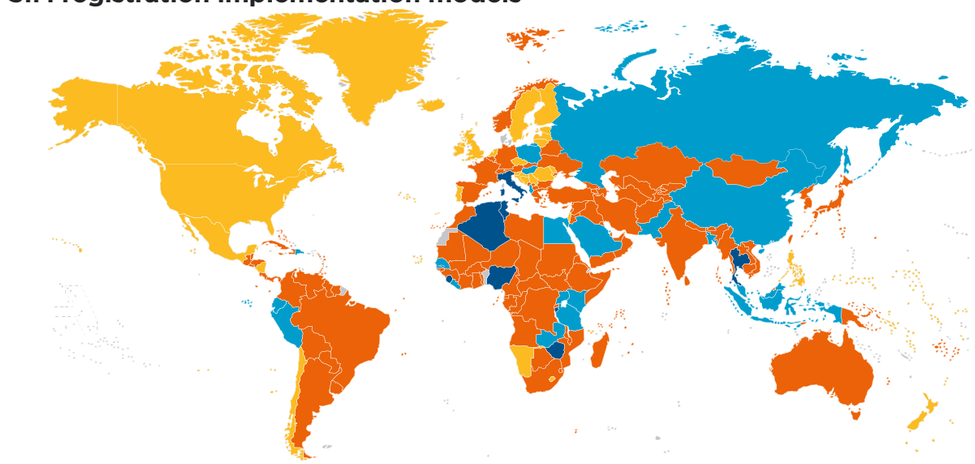
Prepaid SIM registration models can be a barrier to mobile access for consumers

Even though a large proportion of countries globally implement mandatory prepaid SIM registration, governments take widely different approaches to applying proof-of-identity policies. This means that locally licensed MNOs are subject to different requirements in each country, and their investments to fulfil mandatory SIM registration regulations therefore also differ by country. The GSMA has grouped these approaches into three categories:[23]

- **Capture and store:**
  Under this model, MNOs are required to collect and record a user's personal information and proof-of-identity documentation (typically a scanned copy). It is obligatory for MNOs to share their customers' full or partial registration profiles with the government upon request (usually through a warrant). As of December 2020, 'capture and store' is the most popular approach to SIM registration, with 80 per cent of countries using it.[24]
- **Capture and share:**
  In addition to capturing basic information and maintaining a record of their registered customers, MNOs must proactively share full or partial user profiles with the government. Only seven per cent of countries enforce such a model.[25]
- **Capture and validate:**
  MNOs are required to validate a subscriber's identification credentials against a central government database or token (such as a smartcard). Such capabilities typically do not allow MNOs access to additional consumer personal information held by government, but solely enables operators to query a customer's identification credential against the database/token and receive an affirmative or negative response. This would lead to a successful or rejected registration. As of February 2021, 13 per cent of countries follow this approach.[26] Although fewer countries are using the capture and validate model to implement mandatory SIM registration, as more governments digitally transform and develop robust digital identity verification ecosystems, the GSMA anticipates that more countries will adopt this approach, requiring MNOs to digitally verify and authenticate their users.

Figure 4

SIM registration implementation models[27]



23 See the Appendices for the full list of countries.
24 Based on publicly available information.
25 Ibid.
26 Ibid.
27 Based on publicly available information.

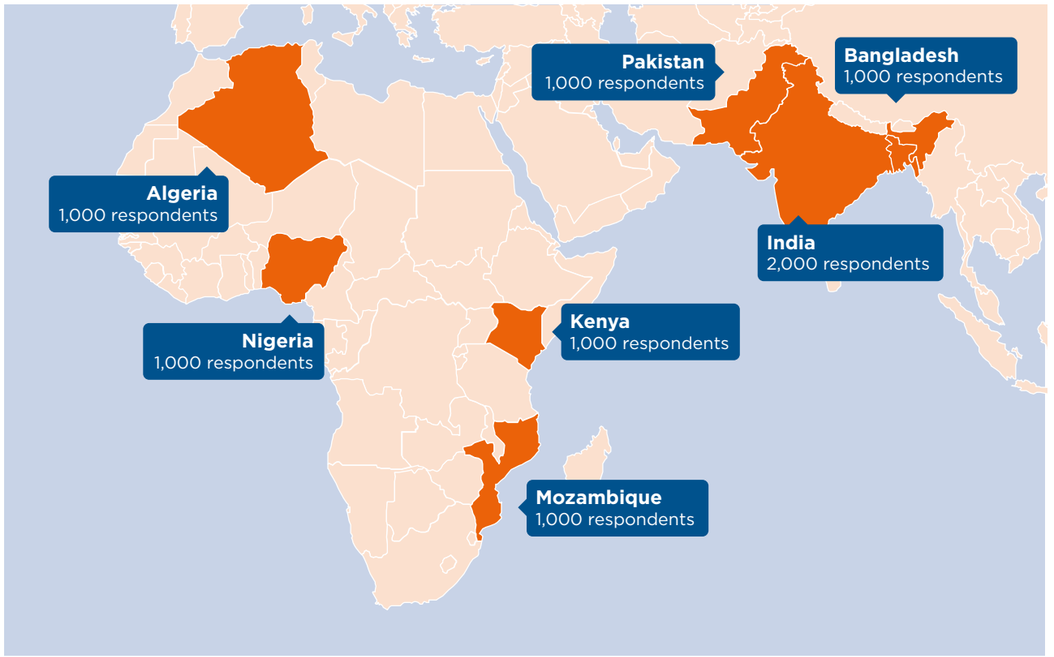
Accessing a SIM card and mobile services in one's name remains a challenge

Recognising that an official form of identification is key to accessing mobile services, especially in countries with mandatory prepaid SIM registration policies, the GSMA Digital Identity programme conducted multi-country consumer research to gauge end-user perceptions around the link between having official ID and accessing mobile services in one's own name.

The research was conducted between September 2020 and January 2021. A face-to-face quantitative survey was conducted with 8,000 individuals in seven LMICs that have a combined population of around 2.1 billion people[28] (see Figure 5). The countries included Algeria, Bangladesh, India, Kenya, Mozambique, Nigeria and Pakistan. The results of the surveys are nationally representative.[29] A summary of some initial findings are presented here, and the full results will be the subject of a standalone report.[30]

Figure 5

GSMA Consumer Survey 2020 sample



The research provides evidence of the barriers individuals face when trying to access a SIM card and mobile services in their own name. A significant barrier emerging from this research is the lack of an official form of identity.

28 Based on UN population data for 2020.
29 See Appendices for the methodology.
30 Report is due to be available in Q2 2021

A national ID card is a strong predictor of whether someone has a SIM card registered in their own name or not

Analysis of questions posed by the Digital Identity programme in the GSMA Consumer Survey 2020[31] (see Figure 6) revealed that certain demographic and socio-economic groups have a significantly higher probability of having a SIM card registered in their own name and, therefore, being able to access personalised and identity-linked mobile services without having to rely on others.

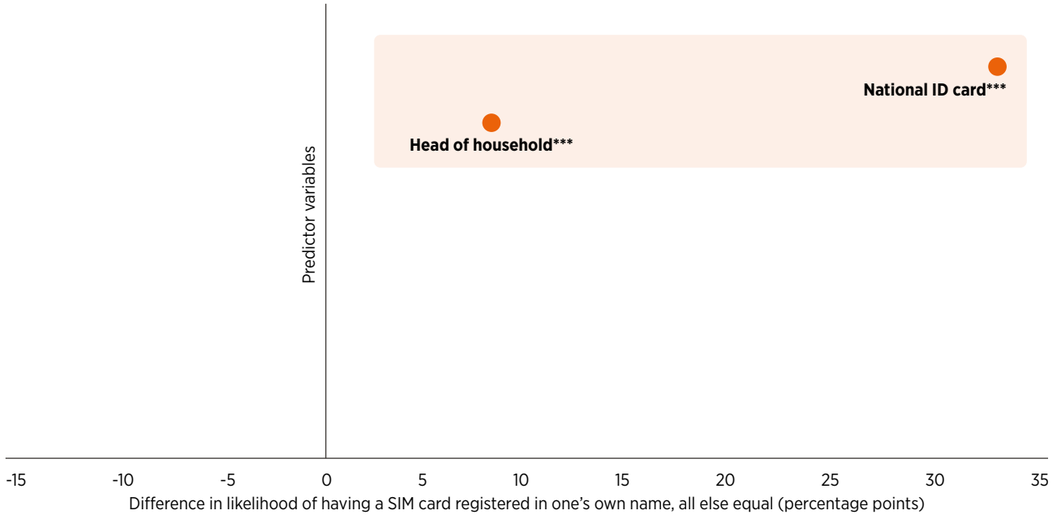
On the positive side, SIM card users who have a national ID card (the most prevalent form of ID found in this survey, and increasingly required for SIM registration and mobile money KYC processes) have a significantly higher probability (by 33 percentage points, p=<0.001) of having a SIM card registered in their own name than SIM card users without a national ID card. This suggests that official ID is a strong and highly significant predictor of access to mobile services in one's own name. So, too, is being the head of a household.[32] Heads of households, in this study, tend to be older males who are literate and have some form of employment.

On the negative side, not having a national ID card and not being head of a household reduces the probability of having a SIM card registered in one's own name.

Figure 6

Predictors of having a SIM card registered in one's own name

(aggregate of seven countries)



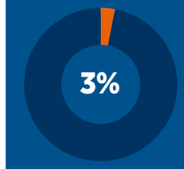
Base: All adult SIM card users aged 18+, n = 6,037 for all seven countries (individual country results may differ). Sample: Nationally representative (Algeria, Bangladesh, India, Kenya, Mozambique, Nigeria and Pakistan). Note: SIM card users are defined as those that have a SIM card (i.e. mobile phone number) that they use at least once a month, in a handset that they have sole or main use of or in other people's handsets. Note: Where an individual presents official ID documents during mandatory SIM registration, and these are accepted, the individual now owns a SIM card registered in their own name. This is different from using a SIM card registered in someone else's name. Note: = *p<0.05, **p<0.01 and ***p<0.001 indicate the significance level of results. Results without a star symbol indicate statistically insignificant variables. Note: These regressions include all seven countries – results may differ by country; variables are binary. Note: Results are marginal effects and have been multiplied by 100 (and rounded to the nearest percentage point) to obtain the percentage point change in the probability of adoption of technology (SIM card registered in one's own name). Results shown are when other relevant socio-economic and demographic factors are controlled for. Source: GSMA Consumer Survey 2020

31 See the Appendices for detailed methodology.

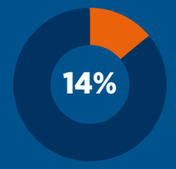
32 A "head of household" is defined as someone who typically makes decisions for the household and they may also be the chief wage earner from paid work or any other form of income.

Many people do not have an official form of identity required for SIM registration

Among the total survey population in the 7 countries covered in this research:



do not have any form of official identity



do not have a national ID card

Official proof of identity is required for mandatory SIM registration of prepaid SIM cards in the seven countries in the GSMA Consumer Survey. As noted earlier, SIM registration requires official forms of identity, such as a digital national ID card (sometimes with biometrics), to register for a SIM card in one's name. However, in practice, different forms of identification can be accepted, particularly since the COVID-19 pandemic when many governments relaxed ID requirements for SIM registration[33] and mobile money KYC.[34,35] This trend is reflected in the results of the GSMA Consumer Survey.

Survey results show that the majority (94 per cent) of respondents have some form of official identity[36] (see Figure 7). Most people have a national ID card (82 per cent), followed by a birth certificate (46 per cent) and another form of ID (21 per cent).[37]

Three per cent of survey respondents did not have any form of official identity. Even though national ID cards/credentials, in a number of countries, are increasingly becoming the only government-recognised documentation permitted for SIM registration and to access to mobile services, 14 per cent of respondents do not have a national ID card. If extrapolated nationally, this is estimated to be around 300 million people[38] in the seven countries surveyed.

33 Lowe, C. and Theodorou, Y. (2021). Commercially sustainable roles for mobile operators in digital ID ecosystems. GSMA.

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

35 See pages 24–33 for a summary of government, MNO and MMP on-boarding relaxations during COVID-19.

36 Government recognised or government issued ID documents which prove who you are, such as birth certificates, national ID cards, or another form of official ID.

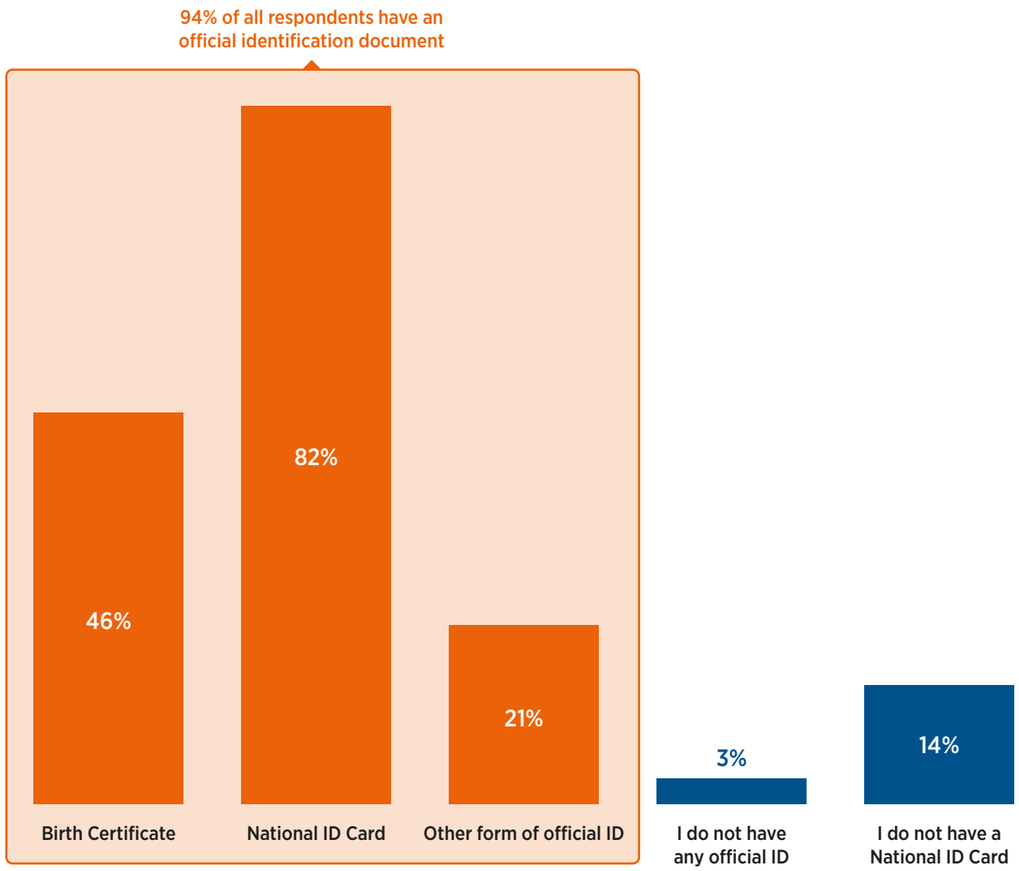
37 Any other government recognised or government issued ID documents aside of a national ID card and a birth certificate. This may typically include a passport, a driver's license or a voter card among some others.

38 Based on UN population data for 2020.

Figure 7

Ownership of an official identification document

Percentage of the total population (aggregate of seven countries)

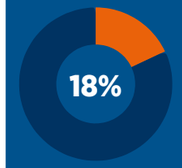


Question: Which, if any, of the following official identification documents do you have? Base: All respondents aged 18+, n = 8,000 for all seven countries aggregated (including those responding with 'prefer not to answer', individual countries may differ). Sample: Nationally representative (Algeria, Bangladesh, India, Kenya, Mozambique, Nigeria and Pakistan) Note: "Other form of official ID" tends to be, among others, a passport, driver's licence or voter card.
Source: GSMA Consumer Survey 2020

ACCESS TO MOBILE SERVICES AND PROOF OF IDENTITY 2021

Lack of official identity is a barrier to registering a SIM/mobile in one's own name

Among SIM card users in the 7 survey countries:



do not have a SIM card registered in their own name

Those with an official form of ID are more likely to have a SIM card registered in their own name than those without one

The GSMA Consumer Survey revealed that 79 per cent of SIM card users have a SIM card registered in their own name. However, 18 per cent do not (Figure 8), and if this is extrapolated nationally, it is estimated that around 285 million people[39] in the seven countries surveyed do not have a SIM card registered in their own name.

In terms of ID, the survey results support the earlier finding (see page 17) that having an official form of identity (a national ID card) is a strong predictor of whether someone has a SIM card registered in their own name or not. The identity gap is clear:

SIM card users that do not have an official form of ID are 56 per cent less likely to have a SIM card registered in their own name than those who have an official form of ID.

The identity gap is similar for a national ID card, but less pronounced. **SIM card users that do not have a national ID card are 33 per cent less likely** to have a SIM card registered in their own name than those who have a national ID card.

Interestingly, a small proportion of SIM card users have managed to register a SIM card in their own name without having an official form of ID. One reason could be that alternative forms of documentation, such as a letter from a village chief vouching for someone's identity, can be accepted for SIM registration. Although this is becoming less common, as some governments (e.g. Nigeria[40]) are now requiring MNOs to re-register all SIM card owners against their national ID number in an effort to drive nationwide enrolment for new national (digital) ID numbers/cards. Yet during the recent pandemic, a number of governments have expanded the range of acceptable IDs to be used for SIM-registration so as to mitigate the risk of exclusion brought about by restrictions on movement.

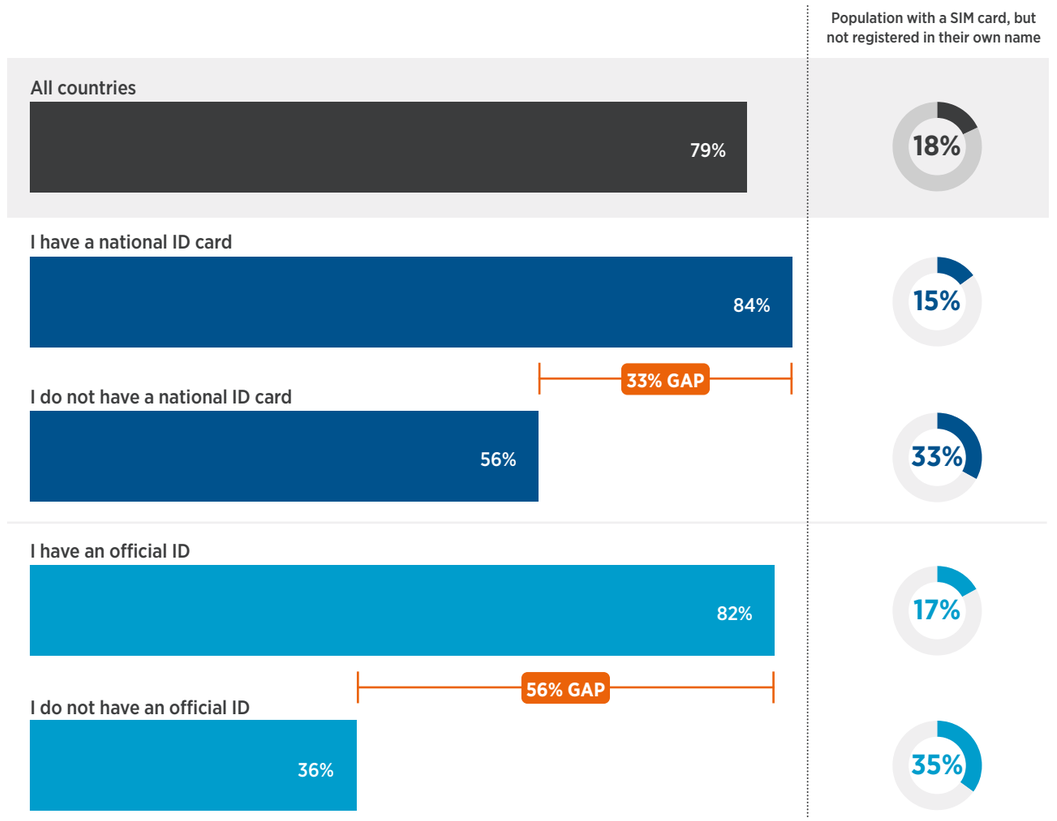
39 Based on UN population data for 2020.

40 National Identity Management Commission. (2 February 2021). Federal Government Lauds Citizens, Extends NIN-SIM Linkage Deadline by 8 Weeks.

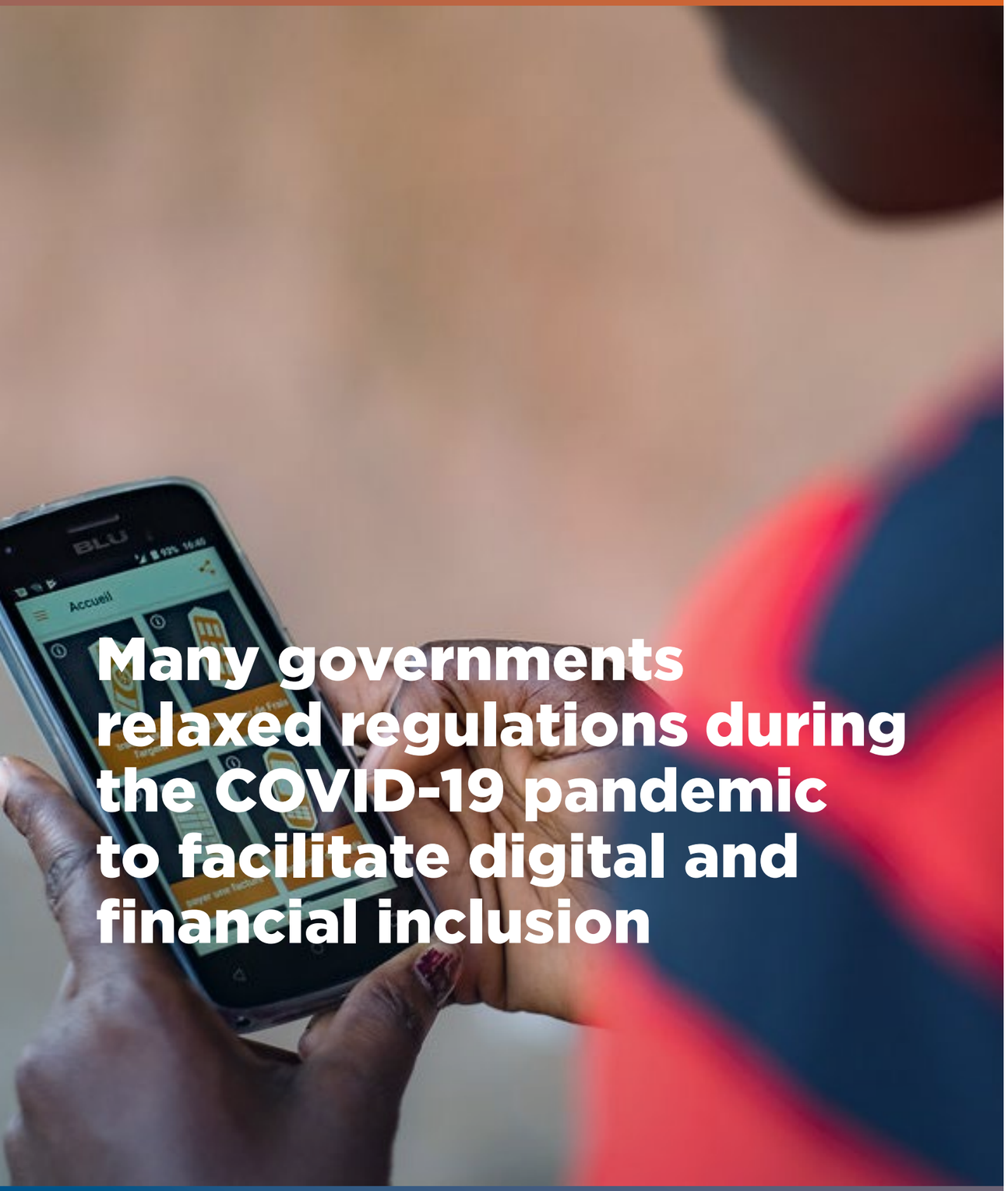
Figure 8

Ownership of a SIM card registered in one's own name, by ID type

Percentage of SIM card using population (aggregate of seven countries)



Question: Typically, when you register a SIM card in your own name you are required to show your ID documents. Do you have a SIM card registered in your name? Base: All adult SIM card users aged 18+, n = 6,037 for all seven countries aggregated (including those responding with 'prefer not to answer', individual countries may differ) Sample: Nationally representative (Algeria, Bangladesh, India, Kenya, Mozambique, Nigeria and Pakistan) Note: SIM card users are defined as those that have a SIM card (i.e. mobile phone number) that they use at least once a month, in a handset that they have sole or main use of or in other people's handsets. Note: Where an individual presents official ID documents during mandatory SIM registration, and these are accepted, the individual now owns a SIM card registered in their own name. This is different from using a SIM card registered in someone else's name. Note: See Appendices for gap calculation. Source: GSMA Consumer Survey 2020



Many governments relaxed regulations during the COVID-19 pandemic to facilitate digital and financial inclusion

Although 157 countries have mandatory SIM registration policies, policymakers in 37 countries introduced and/or adapted a combined total of 93 mobile money related regulations during the COVID-19 pandemic. This was to enable digital and financial inclusion for millions of underserved people[41] who would otherwise have been further marginalised by restrictions on movement and physical contact.

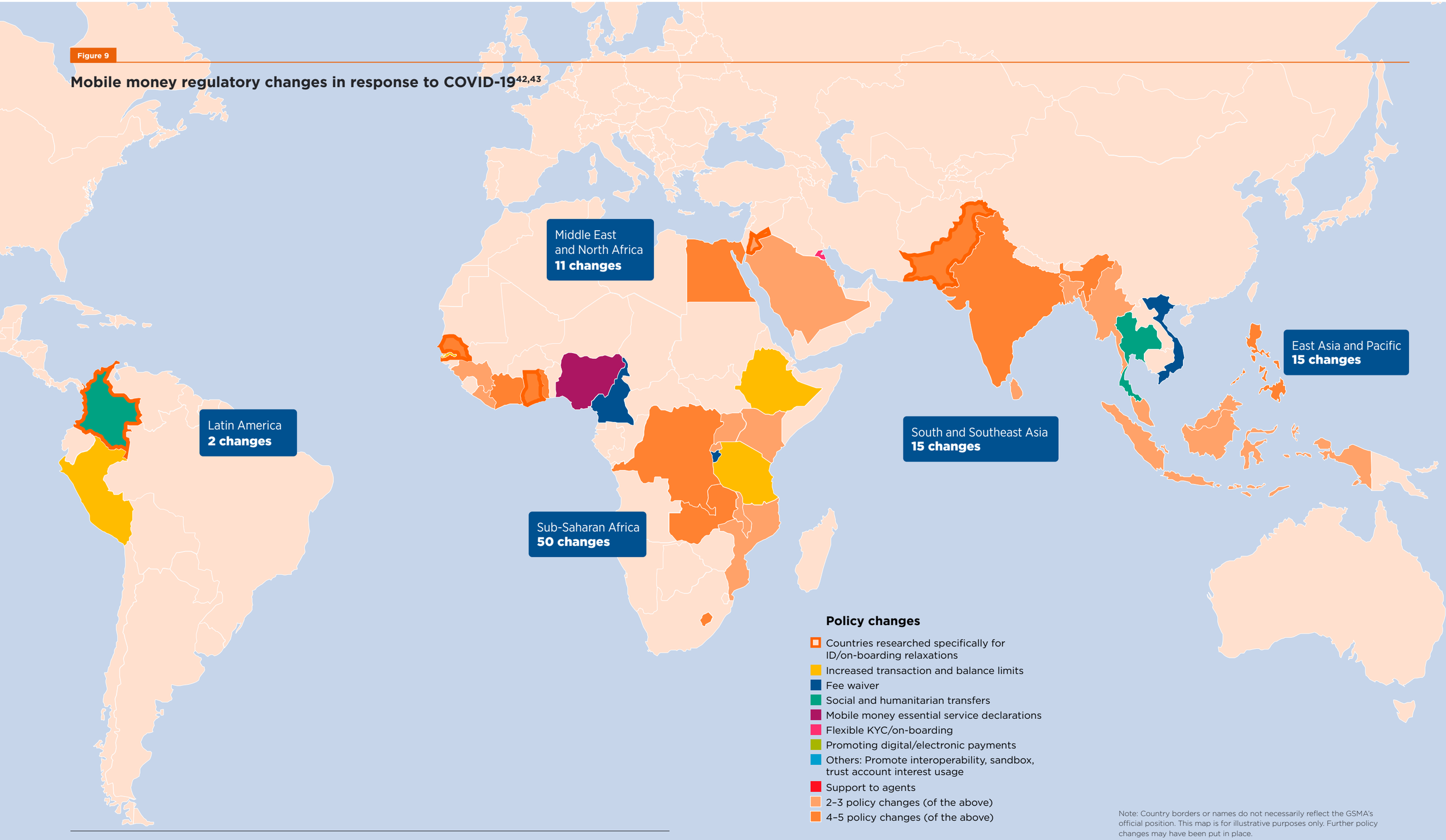
Modifications included classifying mobile money as an essential service, increasing transaction and wallet balance limits and relaxing KYC requirements for on-boarding new customers. These measures enabled agents and providers to continue operating during lockdowns, and promoted adoption and usage of digital financial services.

41 This is based on 'Alliance for Financial Inclusion's (AFI) COVID-19 Member Mitigation Plans', the International Monetary Fund's (IMF) Policy Responses and Chadha, S., Kipkemboi, K. and Muthiora, B. (2019). "Tracking mobile money regulatory responses to COVID-19", GSMA Mobile for Development Blog.

ACCESS TO MOBILE SERVICES AND PROOF OF IDENTITY 2021

Figure 9

Mobile money regulatory changes in response to COVID-19[42,43]



Note: Country borders or names do not necessarily reflect the GSMA's official position. This map is for illustrative purposes only. Further policy changes may have been put in place.

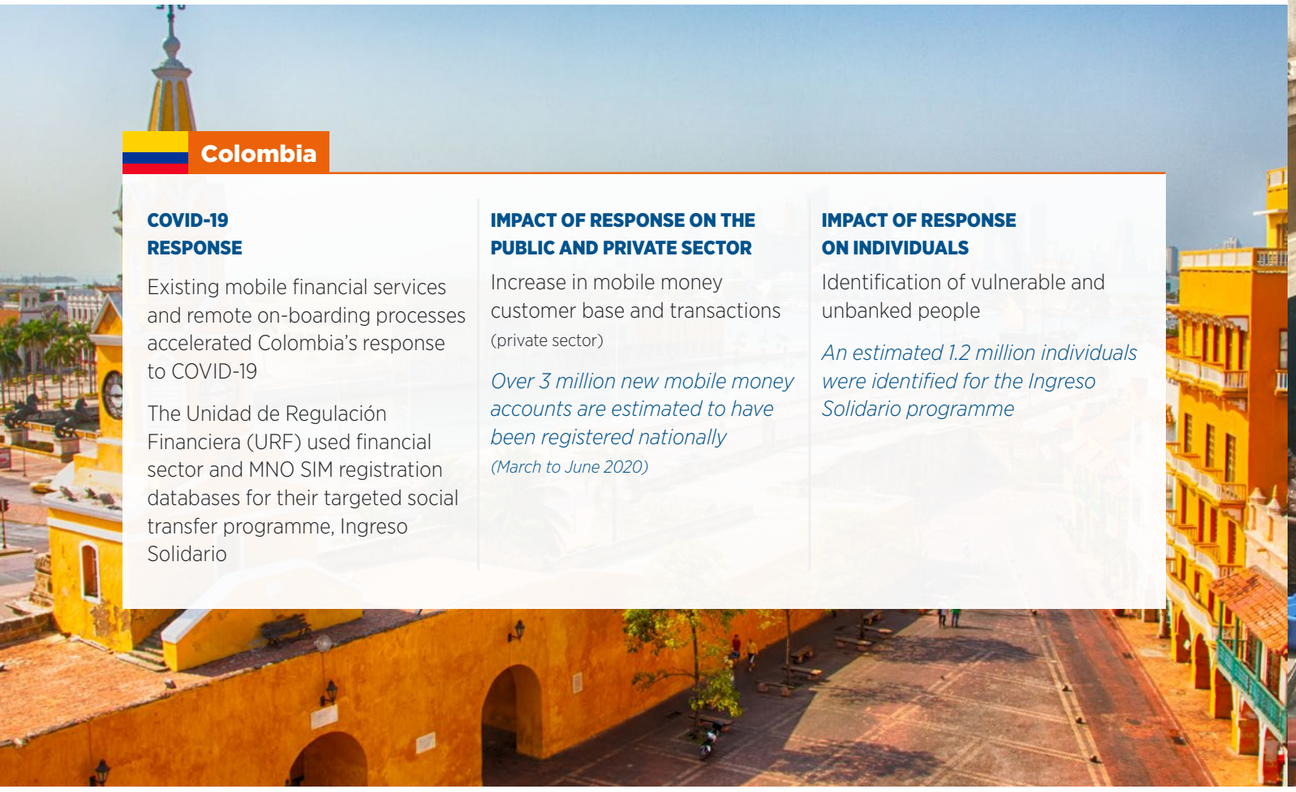
Source: GSMA primary research in 5 countries;
GSMA Mobile Money COVID-19 Regulatory Response Tracker; Desk research

42 See Appendix for the full list of countries.

43 This is based on 'Alliance for Financial Inclusion's (AFI) COVID-19 Member Mitigation Plans', the International Monetary Fund's (IMF) Policy Responses and Chadha, S., Kipkemboi, K. and Muthiora, B. (2019). "Tracking mobile money regulatory responses to COVID-19", GSMA Mobile for Development Blog.

One of these regulatory changes, flexible KYC and on-boarding, was the focus of GSMA Digital Identity programme research due to the link between ID requirements and access to mobile services (i.e. mobile money). The purpose of flexible KYC and on-boarding was to encourage more people to use digital financial services rather than cash, thus reducing contact between mobile money users, agents and merchants.[44] Here, the GSMA conducted exhaustive research with an array of stakeholders from 31 organisations including MNOs, central banks and telecom regulators in five countries to understand how the regulatory changes came about and the early impacts on individuals and the private and public sectors. Since official data on the results and impacts of the changes may not have yet been released, the research findings on regulatory relaxations are based predominantly on evidence from interviews. High-level findings for the five countries are outlined below.[45]

Mobile money KYC regulatory relaxations in response to the COVID-19 pandemic and their impact on the private and public sectors and individuals in five countries[46]



Colombia

COVID-19 RESPONSE

Existing mobile financial services and remote on-boarding processes accelerated Colombia's response to COVID-19

The Unidad de Regulación Financiera (URF) used financial sector and MNO SIM registration databases for their targeted social transfer programme, Ingreso Solidario

IMPACT OF RESPONSE ON THE PUBLIC AND PRIVATE SECTOR

Increase in mobile money customer base and transactions
(private sector)

Over 3 million new mobile money accounts are estimated to have been registered nationally
(March to June 2020)

IMPACT OF RESPONSE ON INDIVIDUALS

Identification of vulnerable and unbanked people

An estimated 1.2 million individuals were identified for the Ingreso Solidario programme

Ghana

COVID-19 RESPONSE

Bank of Ghana (BoG) enabled:

- Existing SIM registration details to be used for on-boarding to basic mobile wallets;
- Increased transaction and account limits; and
- Fee waivers on mobile money transfers and transactions.[47]

A COVID-19 stimulus package was disbursed in part via mobile money

IMPACT OF RESPONSE ON THE PUBLIC AND PRIVATE SECTOR

Increase in customer base, revenue, merchant payments and float balances
(private sector)

Accelerated government e-KYC and Gh-QR code projects

One organisation observed a significant increase in new revenue-generating mobile money accounts
(Q1 to Q4 2020)

IMPACT OF RESPONSE ON INDIVIDUALS

Increased awareness, motivation, user confidence and acceptance of mobile wallets

Increased financial inclusion

Mobile money has become a more widespread and convenient channel for social transfers

44 Ibid.

45 The information shown in Table 1 is limited. More details can be found in the full report: Lowe, C. et al. (2021). Digital identity: accelerating financial inclusion during a crisis. GSMA.

46 The information presented here captures the interview responses, including observations and opinions, of subject matter experts from 31 public and private organisations.

47 Bank of Ghana. (18 March 2020). Bank of Ghana Monetary Policy Committee Press Release.

Jordan

COVID-19 RESPONSE

Central Bank of Jordan (CBJ) permitted:

- Remote on-boarding with simplified KYC to mobile wallets; and
- Removed fees for using other banks' ATMs.

The government used mobile wallets to deliver aid disbursements and salary payments for the National Aid Fund and the National Security Corporation[48]

IMPACT OF RESPONSE ON THE PUBLIC AND PRIVATE SECTOR

Policy relaxations highlighted the importance of digitisation and faster adoption of digital financial services

Online platforms became more robust

Additional customer due diligence (CDD) was required for remote on-boarding

Merchants and agents faced liquidity challenges

Observed a national increase in mobile money customers from 600,000 to 1 million+ (in 2020) and higher revenue for mobile money providers (MMPs)

IMPACT OF RESPONSE ON INDIVIDUALS

Online registration increased the number of individuals opening mobile wallets remotely

Aid and salary payments may have encouraged individuals with no access to financial services to open mobile wallets

Remote on-boarding has led to new services, including JoPACC's Mobile Wallets Gateway[49]

48 See: https://www.cbj.gov.jo/EchoBusV3.0/SystemAssets/627f0da7-e16a-417c-a074-bd59a44b57a9.pdf

49 JOPACC. (n.d.). "Mobile Wallets Gateway".

Pakistan

COVID-19 RESPONSE

State Bank of Pakistan (SBP) enabled:

- Tax waivers to incentivise branchless banking agents to serve customers;
- Removal of interbank and intrabank transfer fees;
- Suspension of biometrics for on-boarding and withdrawals (i.e. cash-out) (two-factor authentication was used instead); and
- Extended biometric reverification deadline for mobile money accounts to the end of 2020.

No transaction limit for trusted merchants (e.g. schools, hospitals, utilities, merchants)[50]

IMPACT OF RESPONSE ON THE PUBLIC AND PRIVATE SECTOR

Cash deposits and transactions declined, but digital transfers and ATM withdrawals increased

MMPs opposed to removal of interbank transfer fees

Removal of interbank transfer fees are thought to be associated with a more than 2× increase in digital fund transfers (2020)

Significant increases in mobile money subscribers are estimated nationally (March/April 2020)

IMPACT OF RESPONSE ON INDIVIDUALS

Increased familiarity with and awareness of mobile financial services

Measures may have saved jobs and allowed continued access to financial services

Essential stores remained open, enabling SIM registration and subsequent access to digital financial services

Individuals benefited from receiving the Prime Minister's COVID-19 relief funds via mobile money

50 State Bank of Pakistan. (18 March 2020). "PSD Circular No. 02 of 2020".

Senegal

COVID-19 RESPONSE

La Banque Centrale des États de l'Afrique de l'Ouest (BCEAO) enabled:

- Existing SIM registration details to be used for simplified on-boarding to basic mobile wallets (app/call centre with name/ID number);
- Free mobile money transfers (<=CFA 5,000);
- Free mobile money water and electricity bill payments (<=CFA 50,000); and
- Increased balance limits on mobile money accounts.

The government used mobile money channels to distribute aid during the pandemic[51]

IMPACT OF RESPONSE ON THE PUBLIC AND PRIVATE SECTOR

Fee waivers have meant lost transaction fee revenue for MMPs

MMPs saw an increase in adoption and use of mobile money

Lower cost of operations for MMPs

13.3 million new mobile money accounts were estimated to have been registered in the BCEAO region

Observed rise in BCEAO regional merchant payments and overall money in the banking system (i.e. deposits), equivalent to CAF 8 billion/$14.4 million

IMPACT OF RESPONSE ON INDIVIDUALS

Faster and more efficient mobile money registration

New mobile offers and services

Improved financial inclusion

Increased awareness and use of mobile money services due to relaxed KYC

Some MNOs supported the UN World Food Programme (WFP) to digitise their food assistance, providing an estimated 40,000+ families with aid to their mobile wallets

51 BCEAO. (2 April 2020). "Avis N° 004-03-2020 relatif aux mesures de promotion des paiements électroniques dans le contexte de la lutte contre la propagation du Covid-19". BCEAO News.

Some mobile operators relaxed on-boarding and ID verification criteria in response to the COVID-19 pandemic and measures imposed by governments

Additional research with MNOs in 31 other countries[52] also shows where MNOs and MMPs have relaxed ID and on-boarding requirements for SIM registration and mobile money KYC in response to COVID-19 (see Figures 10 and 11). Most MNOs and MMPs were required by law to relax their ID and on-boarding requirements, however, some reported that they had put additional measures in place.

Figure 10

MNOs that responded to COVID-19 by relaxing ID verification/on-boarding measures for SIM registration and KYC

Question: In response to COVID-19, have you relaxed on-boarding/verification criteria for SIM registration and KYC? Base: All respondents Source: GSMA Digital Identity MNO survey (2020)

Figure 11

Type of relaxed ID verification/on-boarding measures for SIM registration and KYC implemented by MNOs in response to COVID-19

Question: What are the relaxed measures? Base: MNOs that responded to COVID-19 by relaxing on-boarding/ID verification requirements Source: GSMA Digital Identity MNO survey (2020)

52 See Appendices and the full report: Lowe, C. and Theodorou, Y. (2021). Commercially sustainable roles for mobile operators in digital ID ecosystems. GSMA.

Regulatory relaxations offer opportunities for underserved groups to access mobile services in their own name

Relaxations to SIM registration and mobile money KYC policies in response to COVID-19 were particularly helpful in on-boarding underserved groups to mobile and mobile services.

Some of the most underserved demographic and socio-economic groups are those with **primary education only** (compared to those with secondary, degree and post-graduate education); **women** (compared to men); **persons with disabilities** (compared to persons without disabilities); and those who are **unemployed** (compared to those who are employed).

All of these groups have a significantly lower probability of having a SIM card registered in their own name (see Figure 12) suggesting they are strong predictors of being unable to access mobile services.[53]

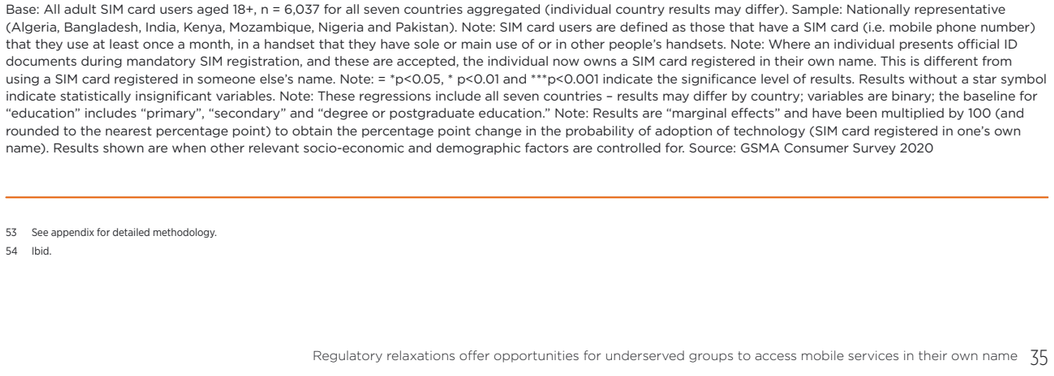
This section examines the prevalence of having a SIM card registered in one's own name among these four populations. It also highlights the gaps between populations, showing how much less likely these four groups are to have their own SIM card and the challenges they face accessing mobile.

Being a woman, having only a primary education, being a person with disabilities and being unemployed, are strong predictors of being less likely to have a SIM card registered in one's own name

Figure 12

Predictors of having a SIM card registered in one's own name

(underserved groups, aggregate of seven countries)[54]



Base: All adult SIM card users aged 18+, n = 6,037 for all seven countries aggregated (individual country results may differ). Sample: Nationally representative (Algeria, Bangladesh, India, Kenya, Mozambique, Nigeria and Pakistan). Note: SIM card users are defined as those that have a SIM card (i.e. mobile phone number) that they use at least once a month, in a handset that they have sole or main use of or in other people's handsets. Note: Where an individual presents official ID documents during mandatory SIM registration, and these are accepted, the individual now owns a SIM card registered in their own name. This is different from using a SIM card registered in someone else's name. Note: = *p<0.05, * p<0.01 and ***p<0.001 indicate the significance level of results. Results without a star symbol indicate statistically insignificant variables. Note: These regressions include all seven countries – results may differ by country; variables are binary; the baseline for "education" includes "primary", "secondary" and "degree or postgraduate education." Note: Results are "marginal effects" and have been multiplied by 100 (and rounded to the nearest percentage point) to obtain the percentage point change in the probability of adoption of technology (SIM card registered in one's own name). Results shown are when other relevant socio-economic and demographic factors are controlled for. Source: GSMA Consumer Survey 2020

53 See appendix for detailed methodology.

54 Ibid.

Underserved group 1

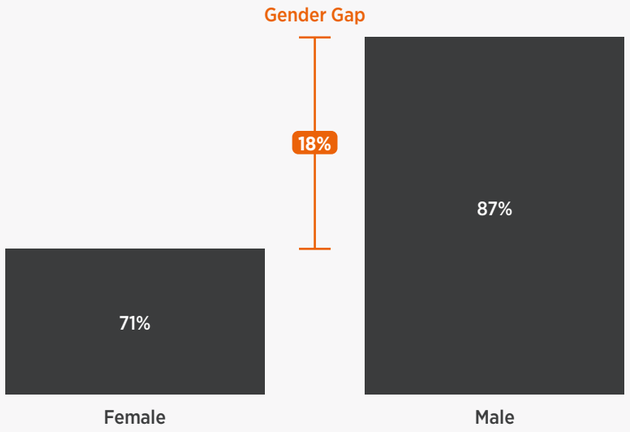
Women

There is a gender gap. Significantly fewer women than men (18 per cent) have a SIM card registered in their own name.

Figure 13

Ownership of a SIM card registered in one's own name, by gender

Percentage of SIM card-using population (aggregate of seven countries)



Question: Typically when you register a SIM card in your own name you are required to show your ID documents. Do you have a SIM card registered in your name? Base: All adult SIM card users aged 18+, n = 6,037 for all seven countries aggregated (individual country results may differ). Sample: Nationally representative (Algeria, Bangladesh, India, Kenya, Mozambique, Nigeria and Pakistan). Note: SIM card users are defined as those that have a SIM card (i.e. mobile phone number) that they use at least once a month, in a handset that they have sole or main use of or in other people's handsets. Note: Where an individual presents official ID documents during mandatory SIM registration, and these are accepted, the individual now owns a SIM card registered in their own name. This is different from using a SIM card registered in someone else's name. Note: See Appendices for gap calculation Source: GSMA Consumer Survey 2020

The GSMA Consumer Survey found, that among SIM card users in the seven countries, significantly fewer women (18 per cent) than men have a SIM card registered in their own name (Figure 13). The research found that about one in four (26 per cent) female SIM card users do not have a SIM card registered in their own name and use someone else's instead.

Not having an ID is a barrier to accessing mobile services in one's own name, but for women, there are also other barriers, for example, because they use a SIM card registered in the name of a family member or friend instead.

In more conservative settings, husbands and other family members often influence what women are permitted to do and possess.[55] Often it is deemed inappropriate for a woman to register a SIM in her own name, and women often face restrictions leaving the household to visit agents, who, in some contexts, are often male.

55 Handforth, C. (2019). Digital Identity Opportunities for Women: Insights from Nigeria, Bangladesh and Rwanda. GSMA.

Underserved group 2

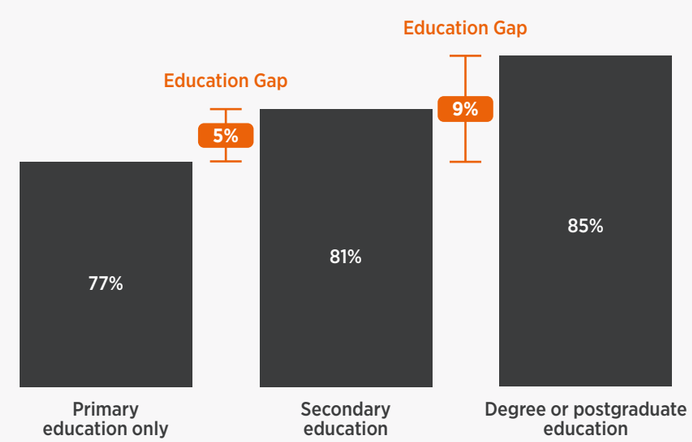
Primary education only

There is an educational gap. Fewer people with primary education only have a SIM card registered in their own name than those who have secondary, degree or postgraduate education.

Figure 14

Ownership of a SIM card registered in one's own name, by level of education

Percentage of SIM card using population (aggregate of seven countries)



Question: Typically when you register a SIM card in your own name you are required to show your ID documents. Do you have a SIM card registered in your name? Base: All adult SIM card users aged 18+, n = 6,037 for all seven countries aggregated (individual country results may differ). Sample: Nationally representative (Algeria, Bangladesh, India, Kenya, Mozambique, Nigeria and Pakistan). Note: SIM card users are defined as those that have a SIM card (i.e. mobile phone number) that they use at least once a month, in a handset that they have sole or main use of or in other people's handsets. Note: Where an individual presents official ID documents during mandatory SIM registration, and these are accepted, the individual now owns a SIM card registered in their own name. This is different from using a SIM card registered in someone else's name. Note: See Appendices for gap calculation Source: GSMA Consumer Survey 2020

Among SIM card users in the seven countries surveyed, having only a primary education is a highly significant predictor of not having a SIM card registered in one's own name. Fewer people with primary education have a SIM card registered in their own name than those who have higher educational qualifications. Those with primary education only are five per cent less likely than those with secondary education to have one, and nine per cent less likely to have one than those with a degree or postgraduate education (see Figure 14). About one in five SIM card users with primary education only (21 per cent) use a SIM card registered in someone else's name.

Aside from ID, the main reason those with only primary education do not have a SIM card registered in their own name is because they use a SIM card registered in the name of a family member or friend instead.

Underserved group 3

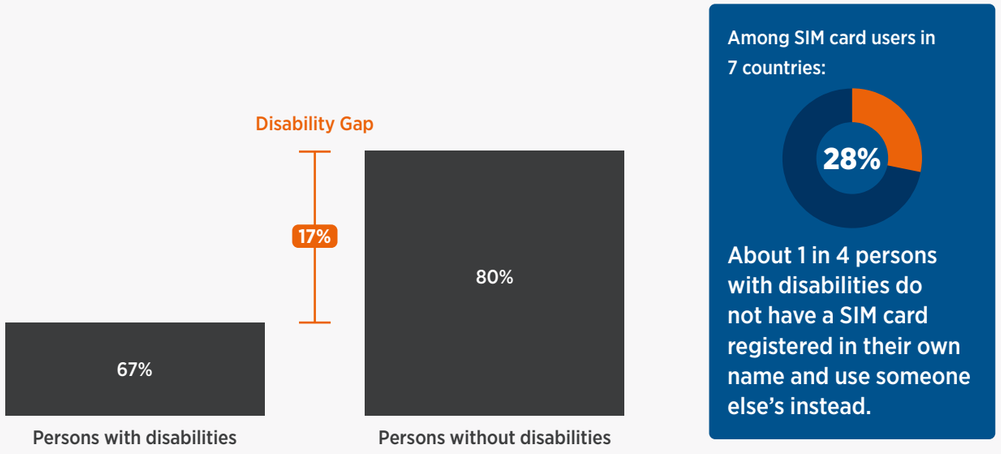
Persons with disabilities

There is a disability gap. Fewer persons with disabilities have a SIM card registered in their own name than those who do not have disabilities.

Figure 15

Ownership of a SIM card registered in one's own name, by disability status

Percentage of SIM card using population (aggregate of seven countries)



Question: Typically when you register a SIM card in your own name you are required to show your ID documents. Do you have a SIM card registered in your name? Base: All adult SIM card users aged 18+, n = 6,037, n = 5,634 for persons without disabilities, n = 403 for persons with disabilities (sample aggregated for all seven countries). Sample: Nationally representative (Algeria, Bangladesh, India, Kenya, Mozambique, Nigeria and Pakistan). Note: SIM card users are defined as those that have a SIM card (i.e. mobile phone number) that they use at least once a month, in a handset that they have sole or main use of or in other people's handsets. Note: Where an individual presents official ID documents during mandatory SIM registration, and these are accepted, the individual now owns a SIM card registered in their own name. This is different to using a SIM card registered in someone else's name. Note: Persons with disabilities are those who responded "cannot do at all" or "a lot of difficulty" to at least one of the functional limitations as stated in the Washington Group Short Set of Questions. Note: see Appendices for gap calculation. Source: GSMA Consumer Survey 2020

Among SIM card users in the seven countries surveyed, being a person with disabilities[56] is a significant predictor of not having a SIM card registered in one's own name. Persons with disabilities are 17 per cent less likely to have one than persons without disabilities (Figure 15). About one in four SIM card users with disabilities (28 per cent) do not have a SIM card registered in their own name and use someone else's instead.

Aside from ID, the main reason persons with disabilities do not have a SIM card registered in their own name is that they use a SIM card registered in the name of a family member or friend.

Persons with disabilities face other barriers[57] that can make it more difficult to access mobile than others, including not being able to register for a SIM card in person. SIM registration often takes place at an MNO agent outlet, retail store or other point of sale (PoS). Sometimes it is necessary to travel long distances to reach these agents, and if a person does not have the appropriate documentation and identification they might be rejected and have to make another journey.

56 A person who reports any acute difficulty ("a lot of difficulty") or complete inability ("cannot do at all") to perform one or more of the functional domains of the Washington Group Short Set of Disability Questions (see Appendices).

57 GSMA. (2020). The Mobile Disability Gap Report 2020.

Underserved group 4

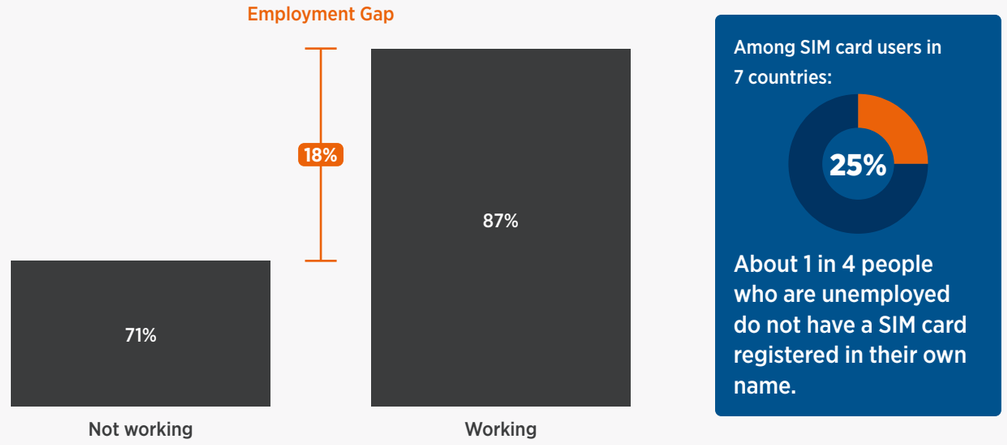
Unemployed

There is an employment gap. Fewer people who are unemployed have a SIM card registered in their own name than those who are employed.

Figure 16

Ownership of a SIM card registered in one's own name, by employment status

Percentage of SIM card using population (aggregate of seven countries)



Question: Typically when you register a SIM card in your own name you are required to show your ID documents. Do you have a SIM card registered in your name? Base: All adult SIM card users aged 18+, n = 6,037 for all seven countries aggregated (individual country results may differ). Sample: Nationally representative (Algeria, Bangladesh, India, Kenya, Mozambique, Nigeria and Pakistan). Note: SIM card users are defined as those that have a SIM card (i.e. mobile phone number) that they use at least once a month, in a handset that they have sole or main use of or in other people's handsets. Note: Where an individual presents official ID documents during mandatory SIM registration, and these are accepted, the individual now owns a SIM card registered in their own name. This is different from using a SIM card registered in someone else's name. Note: See Appendices for gap calculation. Source: GSMA Consumer Survey 2020

Among SIM card users in the seven countries surveyed, being unemployed is a highly significant predictor of not having a SIM card registered in one's own name. Unemployed people are 18 per cent less likely to, when compared with those who are in some form of employment (see Figure 16). This study found that one in four unemployed SIM card users (25 per cent) do not have a SIM card registered in their own name and use someone else's instead.

The main reason, aside from ID, why those who are unemployed do not have a SIM card registered in their own name is that they use a SIM card registered in the name of a family member or friend.

Those who are unemployed also appear to be disproportionately affected by traditional social and cultural norms, where a family member deems it inappropriate to register a SIM card in their own name. They may be more influenced by a male family member or head of household and may not be permitted to register for a SIM card. More female respondents tend to be unemployed than males.

Underserved group 5

Displaced populations including refugees

Displaced populations, including refugees, continue to be at risk of digital and financial exclusion

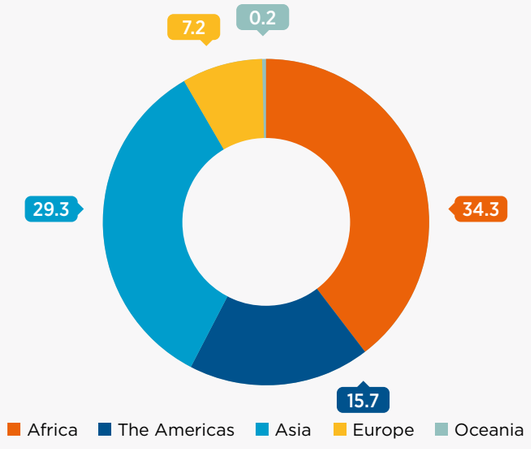
In 2021, the United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA) expects that 235 million people worldwide will need humanitarian assistance and protection.[58] Trends suggest that mobile technology will play a greater role in meeting this growing need, and the GSMA's research has shown that the number of countries implementing proof-of-identity requirements to access mobile services is also increasing. Considering the circumstances under which forcibly displaced persons (FDPs) flee their homes, they are often unlikely to possess the identity documentation needed to meet proof-of-identity requirements and, consequently, access life-saving assistance.

According to the UNHCR 2019 Global Trends report,[59] at the end of 2020 there were 185[60] countries hosting 86.5 million persons of concern. UNHCR, the UN Refugee Agency, classifies persons of concern as refugees, returnees, stateless people, internally displaced persons (IDPs) and asylum seekers. These same classifications are used in this report. The region hosting the highest number of persons of concern is Africa, with 34.3 million individuals, followed by Asia at just under 30 million.

Seventy-eight per cent of countries (144) that host persons of concern also enforce mandatory SIM registration while 50 per cent of host countries (93) offer mobile money services.

Figure 17

Persons of concern (million) by host region[61]



58 UN OCHA. (1 December 2020). "UN and Partners Release Record Humanitarian Response Plan as COVID-19 Wreaks Havoc". Global Humanitarian Overview 2021.

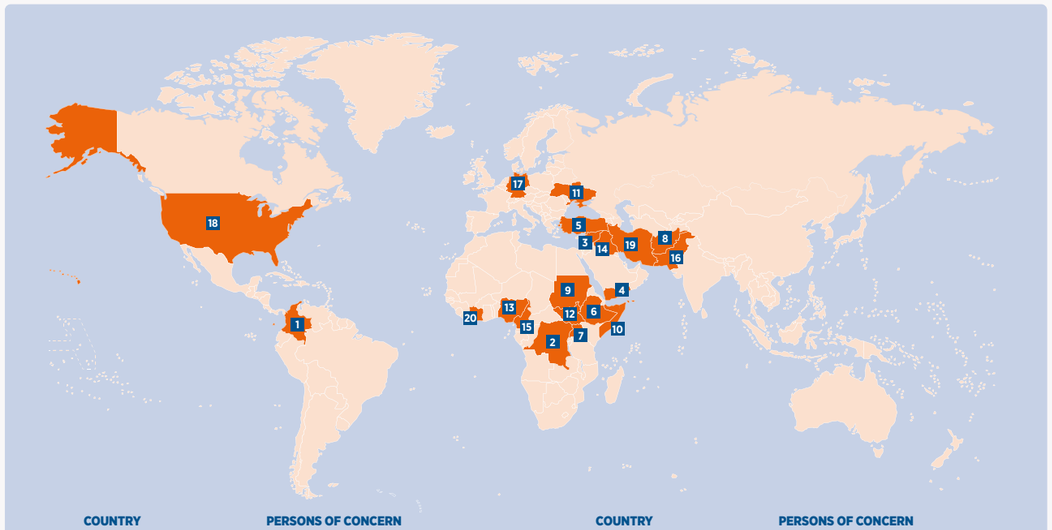
59 UNHCR. (2020). Global Trends: Forced Displacement in 2019.

60 Serbia and Kosovo are included in the countries that host persons of concern, but the persons of concern have been excluded from the calculations. This is because it is joint country data and difficult to treat separately.

61 Based on information from UNHCR's Global Trends 2019 data.

Figure 18

Top 20 Host Countries for Persons of Concern[62]



	COUNTRY	PERSONS OF CONCERN		
1	Colombia	10.2m	✓	✓
2	Democratic Republic of Congo	7.70m	✓	✓
3	Syria	6.94m	✓	
4	Yemen	3.97m	✓	
5	Turkey	3.91m	✓	✓
6	Ethiopia	3.77m	✓	✓
7	Uganda	3.69m	✓	✓
8	Afghanistan	3.08m	✓	✓
9	Sudan	2.96m	✓	✓
10	Somalia	2.71m	✓	✓
11	Ukraine	2.45m	✓	
12	South Sudan	2.35m	✓	✓
13	Nigeria	2.27m	✓	✓
14	Iraq	2.18m	✓	✓
15	Cameroon	1.71m	✓	✓
16	Pakistan	1.53m	✓	✓
17	Germany	1.47m	✓	
18	United States of America	1.19m		
19	Iran	0.98m	✓	✓
20	Côte d'Ivoire	0.96m	✓	✓

✓ Implements SIM registration ✓ Offers mobile money services

A large majority of persons of concern are hosted in 20 countries (see Figure 18). Nineteen of these countries enforce mandatory SIM registration, which means that 64.1 million persons of concern must provide proof of identity to access mobile services. Similarly, approximately 50 million persons of concern in 15 of the top 20 host countries may be able to access mobile money services with the requisite ID.

62 Based on information from UNHCR's Global Trends 2019 data and GSMA data.

Refugees

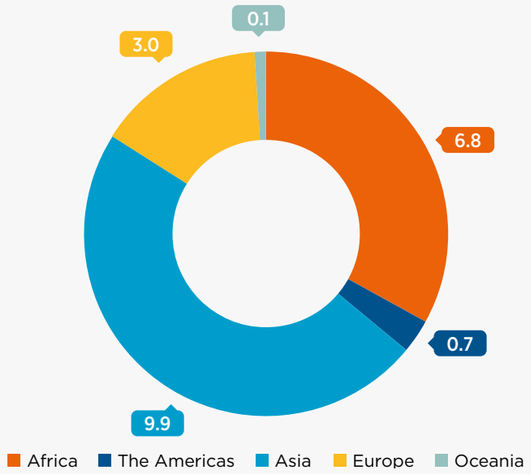
Refugees account for 24 per cent of persons of concern.

The GSMA finds that:

- Globally, 172 countries host 20.4 million refugees and people in refugee-like situations[63].
- The regions hosting the most refugees are Asia (9.9 million) and Africa (6.8 million) (see Figure 19).
- Seventy-nine per cent of countries hosting refugees (136) mandate SIM registration.
- Fifty per cent of countries hosting refugees (86) offer mobile money services.

Figure 19

Refugees (million) by host region

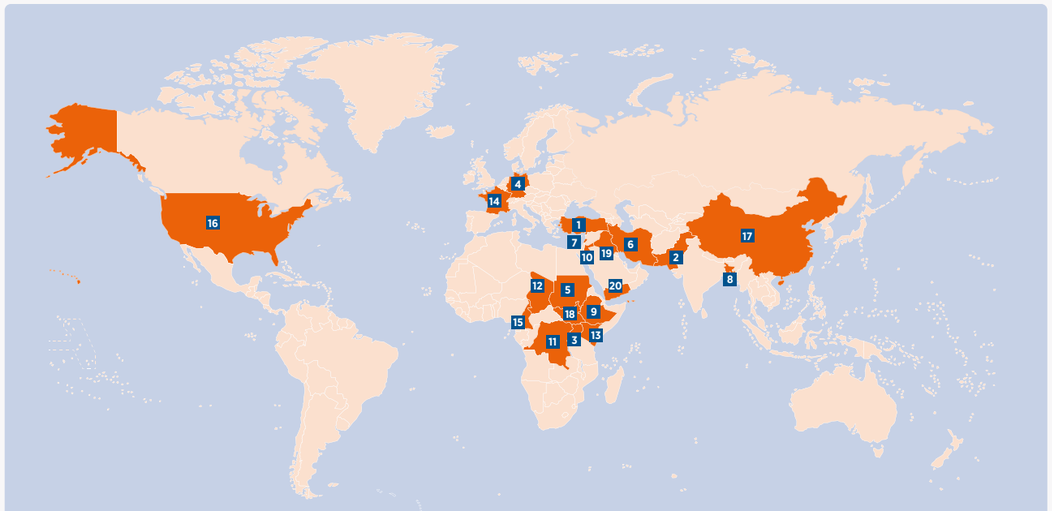


- Eighty per cent of refugees and people in refugee-like situations are hosted by 20 countries. Nineteen of these host countries have implemented mandatory SIM registration, which means 16.1 million refugees have the potential to be digitally and financially included if they have identity documentation that is deemed acceptable by the host government.
- Fourteen of the top 20 host countries offer mobile money services, which gives 13 million persons of concern the opportunity to access digital financial services.

63 "The category of people in a refugee-like situation is descriptive in nature and includes groups of people who are outside their country of origin and who face protection risks similar to those of refugees, but for whom refugee status has, for practical or other reasons, not been ascertained" https://reporting.unhcr.org/glossary/r

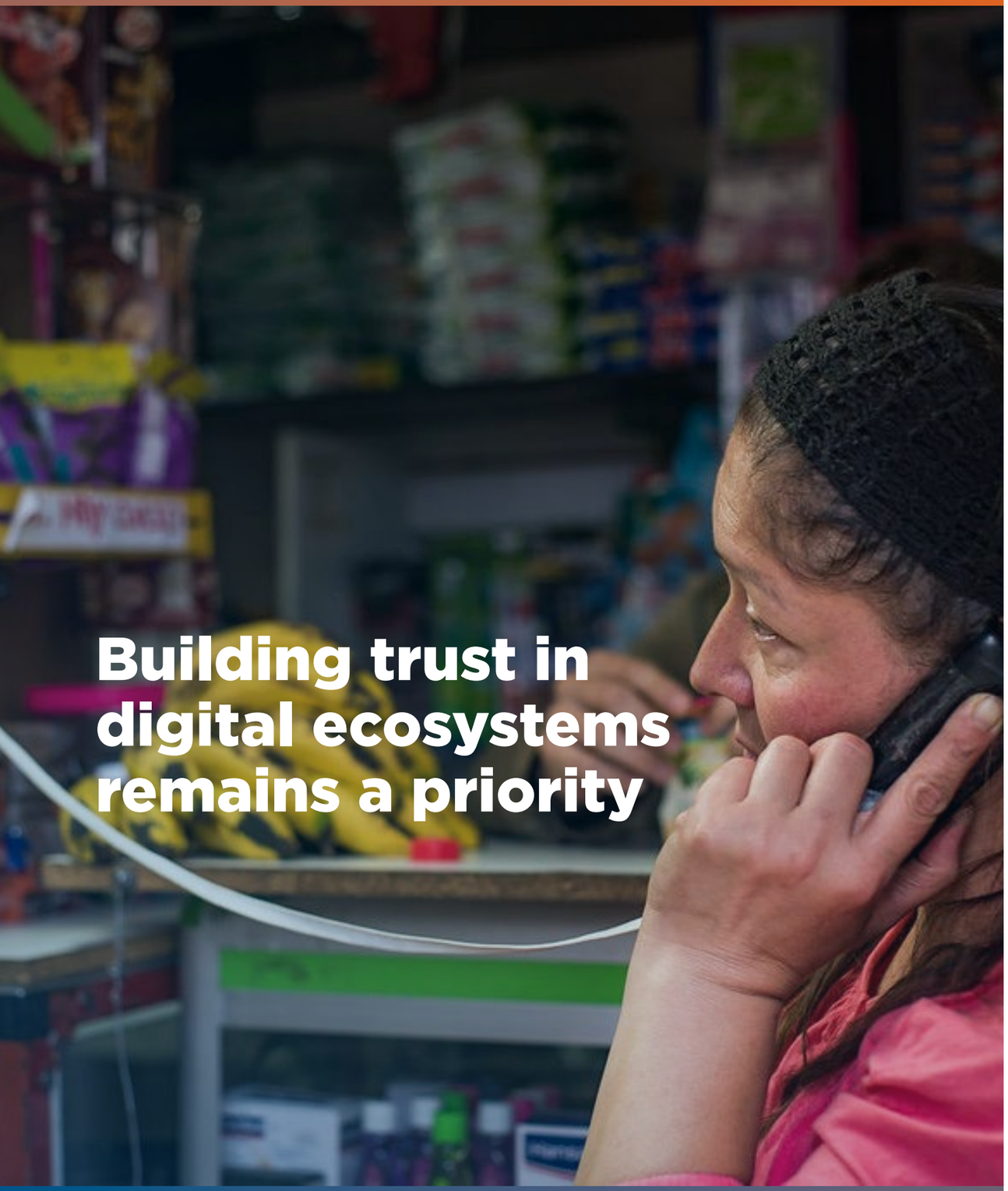
Figure 20

Top 20 refugee host countries



	COUNTRY	PERSONS OF CONCERN		
1	Turkey	3.58m	✓	✓
2	Pakistan	1.42m	✓	✓
3	Uganda	1.36m	✓	✓
4	Germany	1.15m	✓	
5	Sudan	1.06m	✓	✓
6	Iran	0.98m	✓	✓
7	Lebanon	0.92m	✓	
8	Bangladesh	0.85m	✓	✓
9	Ethiopia	0.73m	✓	✓
10	Jordan	0.69m	✓	✓
11	Democratic Republic of Congo	0.52m	✓	✓
12	Chad	0.44m	✓	✓
13	Kenya	0.44m	✓	✓
14	France	0.41m	✓	
15	Cameroon	0.41m	✓	✓
16	United States of America	0.34m		
17	China	0.30m	✓	
18	South Sudan	0.30m	✓	✓
19	Iraq	0.27m	✓	✓
20	Yemen	0.27m	✓	

Implements SIM registration Offers mobile money services



Building trust in digital ecosystems remains a priority

Data protection and data privacy frameworks are key to building consumer trust in digital services. As more individuals turn to digital services, it is imperative that governments ensure appropriate frameworks are in place to handle consumer data, especially in countries that impose mandatory SIM registration.

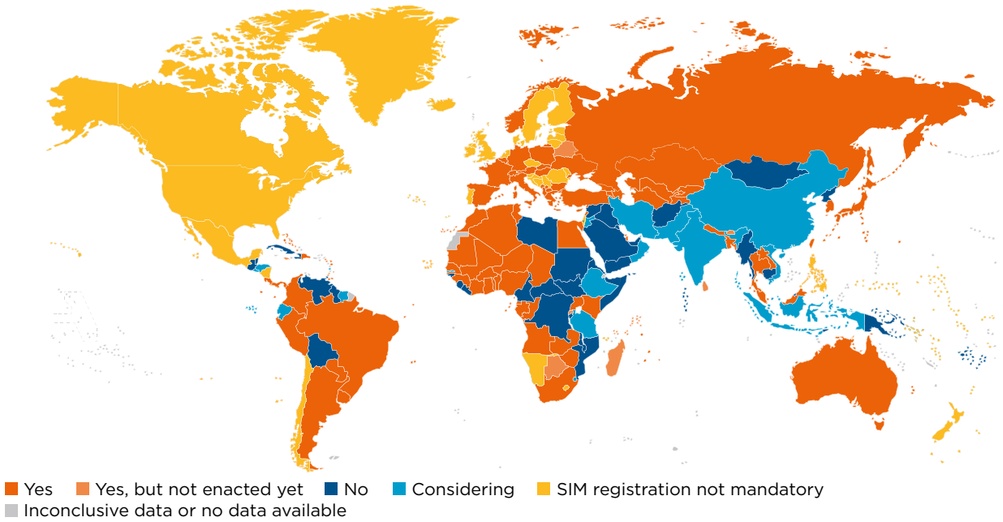
Although many of the countries mandating SIM registration maintain a data protection and/or privacy framework (64 per cent), there is still a significant proportion of countries that are either considering introducing a data protection and/or privacy framework or do not have one at all. The GSMA Digital Identity programme has been tracking this metric in this report series since 2017.

The GSMA found that:[64]

- In Africa, 14 countries enforcing mandatory SIM registration do not have a data protection or privacy framework. Four countries enforcing mandatory SIM registration are considering the implementation of a data protection framework, and one country that is considering introducing SIM registration is also actively considering introducing a data protection or privacy framework.
- In the Americas, eight countries enforcing mandatory SIM registration do not have a data protection or privacy framework. Four countries that enforce mandatory SIM registration are actively considering introducing a data protection or privacy framework.
- In Asia, 15 countries enforcing mandatory SIM registration do not have a data protection or privacy framework. Eight countries in the region that enforce mandatory SIM registration are also considering introducing a data protection or privacy framework.
- In Oceania, three countries enforcing mandatory SIM registration do not have a data protection or privacy framework. While one country is considering introducing SIM registration, it does not maintain a data protection or privacy framework and is not actively considering one.

Figure 21

State of data protection/privacy frameworks in countries mandating SIM registration[65]



64 See the Appendices for the full list of countries.

65 Based on information from 'One Trust Data Guidance'; and 'DLA Piper', 'Privacy Matters'.

Conclusion and policy recommendations

COVID-19 has highlighted the role of mobile in keeping people connected during a crisis. Having a mobile SIM card (and a mobile money account) registered in one's own name has proven to be vital for users to receive social protection payments, manage their health records and access benefits or services that may be unique to their personal circumstances.

Proof of identity is key to being able to register for mobile services in one's own name. SIM card users who have an official ID[66] are twice as likely (as users who do not have one) to have a SIM card registered in their name. While this is prevalent in the 157 countries mandating SIM registration, those most impacted by these policies are underserved populations in LMICs, notably women, persons with disabilities, those with only primary education, the unemployed and forcibly displaced persons, such as refugees. The risk of digital and financial exclusion is therefore much higher among these population segments.

Research findings showed that governments in 37 countries relaxed regulatory policies around mobile services including how new customers can be on-boarded. These actions were taken during the COVID-19 pandemic to mitigate the risk of underserved groups being further marginalised by lockdown and restrictions on movement and physical contact.

Just over a third (37 per cent) of countries mandating SIM registration have no or inadequate privacy/data protection frameworks. This can leave consumers with limited, if any, rights to seek legal redress for the exploitation of their privacy or personal data. This could not only lead to consumer calls for greater transparency in the use of personal data, but also make consumers less willing to register a SIM in their own names or adopt identity-linked mobile services. Being transparent with consumers about how their data is used is important for maintaining high levels of trust in digital and mobile ecosystems.

Based on these conclusions and the research insights shared in this report, **the GSMA encourages governments mandating (or considering mandating) prepaid SIM registration to:**

Establish inclusive (digital) identification ecosystems based on internationally accepted principles,[67] empowering all individuals within their jurisdiction to access an official or recognised form of identification, in line with UN Sustainable Development Goal (SDG) 16.9.[68]

Consider (for example, while COVID-19-related restrictions are in place) temporarily **relaxing[69] proof-of-identity requirements** for SIM registration and **promoting electronic/remote ID verification** where this capability can be easily developed or offered to MNOs.

66 Government-recognised or government-issued ID documents that prove who you are, such as a birth certificate, national ID card or another form of official ID.
67 Theodorou, Y. (4 March 2021). "10 Principles for Good ID: A 2020 Refresh". GSMA Mobile for Development Blog.
68 See SDG 16: https://sdgs.un.org/goals/goal16
69 Financial Action Task Force (1 April 2020). Statement by the FATF President: COVID-19 and measures to combat illicit financing.

Where mobile money services are offered, consider **simplifying customer on-boarding processes** by enabling MNOs to use customers' SIM registration data to open a basic mobile money wallet (i.e. harmonisation of SIM registration with mobile money KYC requirements). This practice can help more underserved groups to receive social benefits remotely and, ultimately, be financially included.

Adopt a **risk-based approach**[70] when imposing KYC measures (for accessing mobile financial services), balancing the dual objectives of enabling greater access for underserved populations and mitigating the risk of such measures being exploited to aid money laundering, terrorist financing and other forms of criminal activity.

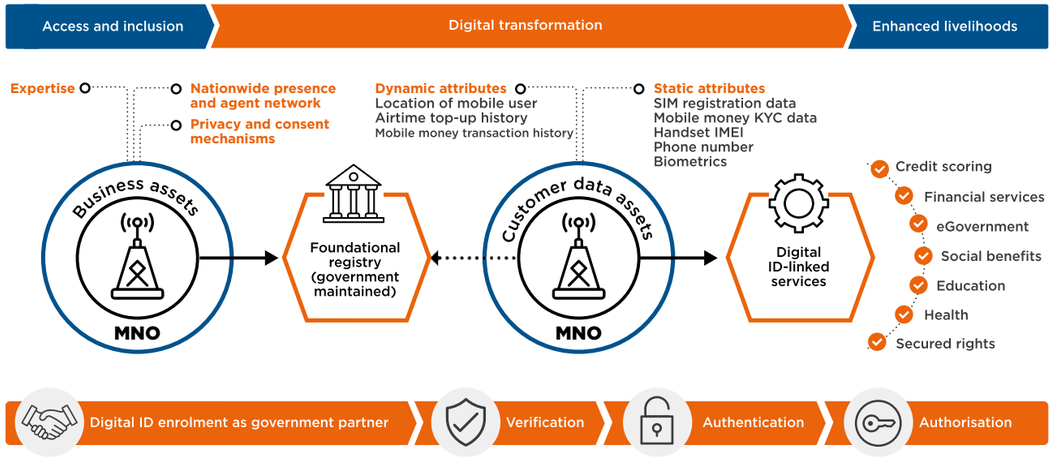
Introduce **policy incentives** (such as targeted social protection programmes) and **support initiatives** aimed at promoting the digital and financial inclusion of underserved groups.

Enact or strengthen **privacy and data protection frameworks** that foster trust in digital ecosystems.

Seek opportunities to work in partnership with MNOs, leveraging their assets to address public policy objectives. For example, partnering to accelerate national ID enrolment efforts, developing simplified and digital on-boarding processes for SIM registration and KYC or creating demand for e-government services by supporting mobile-linked identity verification solutions to unlock access to civic participation (tax, voting, education, etc.). Such partnerships[71] may also focus on providing access to life-enhancing mobile services for remote, poor and underserved communities, in more impactful, cost-effective, efficient and transparent ways.[72]

Figure 22

Roles that MNOs can play in supporting digital ID ecosystems



70 FATF/OECD. (2020). Guidance on Digital Identity.

71 Theodorou, Y. (29 April 2020). "GSMA Digital Identity Programme: Insights and Achievements 2016–2020". GSMA Mobile for Development Blog.

72 Lowe, C. and Theodorou, Y. (2021). Commercially sustainable roles for mobile operators in digital ID ecosystems. GSMA.

Appendices

Methodology

GSMA Digital Identity COVID-19 Know Your Customer Policy Relaxation Research (2020)

Certain insights presented in this report are based on in-depth interviews with 56 senior stakeholders and subject matter experts from 31 public and private sector organisations in five countries (Colombia, Ghana, Jordan, Pakistan and Senegal), conducted in Q4 2020. The organisations interviewed include central banks, financial institutions, mobile money providers (MMPs), mobile network operators (MNOs), government ID authorities, government departments and regulators.

This research was conducted to better understand mobile money Know Your Customer (KYC)-related policy relaxations (linking ID to digital and financial inclusion) made by governments in response to the COVID-19 pandemic and their impacts on individuals and organisations.

The full report can be found here:

Digital Identity: Accelerating Financial Inclusion During a Crisis

GSMA Digital Identity Mobile Network Operator Survey (2020)

Certain insights presented in this report are based on an in-depth survey and interviews with a sample of MNOs in 31 countries, conducted in Q3 and Q4 2020. This research investigates the ID verification landscape, predominantly in low- and middle-income countries (LMICs), and focuses on ID verification in SIM registration and mobile money KYC processes. The research considers the ecosystems, benefits, opportunities, costs and threats of ID verification for MNOs, and it 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, 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.

The full report can be found here:

Commercially Sustainable Roles for Mobile Operators in Digital ID Ecosystems

GSMA Consumer Survey (2020)

Certain consumer insights presented in this report are based on a nationally representative survey conducted in seven LMICs (Algeria, Bangladesh, India, Kenya, Mozambique, Nigeria and Pakistan) that were part of the broader Consumer Insights Survey conducted annually by the GSMA. Fieldwork was conducted between Q4 2020 and Q1 2021. In all countries, a nationally representative sample of the adult population aged 18 and over was selected. At least 1,000 face-to-face interviews were conducted in each country surveyed, with 2,000 interviews conducted in India. This research aimed to unpack consumer usage of, and attitudes towards, official identity, digital identity, SIM cards registered in one's own name, MNO-provided ID verification and mobile services and ID-linked mobile-enabled benefit transfers. Full survey results and country-level analysis will be the subject of a separate report.

Sampling and fieldwork

In all countries, a nationally representative sample of the adult population aged 18 and over was surveyed. A minimum of 1,000 interviews were conducted in each country, with 2,000 interviews undertaken in India.

To achieve a nationally representative sample, quotas were applied in line with census data (or other appropriate sources) on the following metrics:

- Age category by gender;
- Urban and rural distribution by gender;
- Region/state; and
- Socio-economic class (SEC) to ensure a representative segment of lower income respondents (no such quota was applied in Mozambique in the absence of reliable SEC profiling data).

While a quota was not applied to education (other than where it contributed to SEC classification), it was tracked regionally and nationally during and after the fieldwork as an important indicator of a representative sample.

Sampling points where interviews were conducted were distributed proportionately between urban and rural areas in accordance with census data and national statistics offices. To achieve wide geographical coverage and reduce the effects of clustering, a minimum of 100 sampling points were used in each country (200 in India).

This research used a mix of purposive and random sampling approaches. Depending on the country, sampling points were either randomly distributed – with an administrative area's probability of selection proportionate to the size of its population (random sampling) – or selected to reflect the linguistic, cultural and economic variations of each country (purposive sampling). Local experts and national statistics offices checked the sampling frames to ensure they were valid and representative.

The survey was delivered via interviewer-administered, computer-assisted personal interviewing (CAPI). Survey interviews were conducted in the local language(s) by both female and male interviewers. Interviews were conducted at respondents' homes. Within sampling points, systematic random routes were used for residence selection.

Weights were applied to the data using a random iterative method (RIM) whereby several non-interlocking quotas were applied in an iterative sequence and repeated as many times as needed for the quotas to converge. This corrected any imbalances in the profiles, although weightings (and the resulting impact on effective sample sizes) were minimised as much as possible by controlling key quota variables over the course of the fieldwork.

The sampling approach was designed to achieve full national representativeness where practical; however, some more remote rural areas or regions with ongoing unrest or security concerns were excluded from sampling. This may have had an impact on results, especially since mobile phone coverage, access and use will be different, and likely most limited, in these areas, particularly for women.

As a consequence of the coronavirus pandemic no interviewing was conducted inside a home, with interviewing instead taking place on the doorstep or other appropriate location. All necessary precautions were taken to ensure the safety of interviewers and respondents to comply with guidelines issued (e.g. sanitising of materials and use of PPE).

As with all survey data, the results are subject to sampling error (typically ± 2–3%), as well as other potential sources of error. It is also important to recognise that fieldwork took place during the coronavirus pandemic and this created challenges in accessing some areas, leading to extended fieldwork periods.

Analysis of the research

Calculating adoption and usage gaps

A primary objective of the study was to understand the extent of the adoption and gaps around official ID and SIM cards registered in one's own name, as well as usage and attitudes of MNO-provided ID verification and mobile services. In order to calculate an accurate representation of the size of the gap between different demographic and socioeconomic groups in each country, the following formula was applied:

$$\frac{\%\ \text{Group 1 ownership/usage} - \%\ \text{Group 2 ownership/usage}}{\%\ \text{Group 1 ownership/usage}}$$

This shows the gap in ownership or usage relative to ownership or usage in a comparison group.[73]

Regression analysis

Observed rates of technology ownership, digital identity adoption and usage of services on mobile phones give us a picture of access and adoption according to different demographic and socioeconomic factors. The degree to which these factors (such as age, income, education, geography, etc.) explain the access gaps is best explored through regression analysis, which can be used to analyse the data from the seven countries included in the 2020 survey.[74]

These dependent variables are binary and are defined as:

$$y_i \begin{cases} 1 \text{ if the } i\text{th individual has use or access to the technology/service} \\ 0 \text{ if the } i\text{th individual does not have use or access to the technology/service} \end{cases}$$

These regressions assess the key drivers of adoption of official ID and SIM cards registered in one's own name, as well as usage and attitudes of MNO-provided ID verification and mobile services based on a combination of socio-economic and demographic characteristics. By using this suite of variables for the observable drivers of mobile adoption (e.g. education levels, age, employment, rural-urban location), the coefficient for each variable should represent the effect of that factor while the other socioeconomic and demographic factors are controlled for. The 'marginal effect' associated with the coefficient for each variable quantifies the effects as a percentage impact of each factor on the probability of adoption of official ID and SIM cards registered in one's own name, as well as usage and attitudes of MNO-provided ID verification and mobile services.

73 In reporting observed statistics, the analysis adheres to subgroups with a minimum sample size of n=30.

74 Further details on the econometric framework can be found in the following paper on disaggregating the drivers of mobile technology adoption: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748717

Policy landscape, by country

Africa

	SIM registration mandated	SIM registration under consideration	SIM registration not mandated	State of SIM registration inconclusive	'Capture and Store' SIM user information	'Capture and Share' SIM user information	'Capture and Validate' SIM user information	Mandate SIM registration and have a data privacy framework	Mandate SIM registration but lack a data privacy framework	Mandate or considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework	Considering SIM registration and are considering a data privacy framework
Algeria	✓					✓		✓					
Angola	✓				✓			✓					
Benin	✓					✓		✓					
Botswana*	✓				✓			✓					
Burkina Faso	✓				✓			✓					
Burundi†	✓					✓			✓				
Cabo Verde		✓									✓		
Cameroon†	✓		✓		✓				✓				
Central African Republic	✓				✓				✓				
Chad	✓				✓			✓					
Comoros													
Congo	✓				✓			✓					
Congo, Dem. Republic†	✓				✓				✓				
Côte d'Ivoire†	✓				✓			✓					
Djibouti				✓									
Egypt†	✓						✓	✓					
Equatorial Guinea	✓				✓			✓					
Eritrea	✓				✓				✓				
Eswatini	✓				✓					✓			
Ethiopia†	✓				✓					✓			
Gabon	✓				✓			✓					
Gambia†	✓					✓				✓			
Ghana†	✓				✓			✓					
Guinea†	✓				✓			✓					
Guinea-Bissau	✓				✓				✓				
Kenya†	✓						✓	✓					
Lesotho†		✓										✓	
Liberia†	✓						✓		✓				
Libya	✓				✓				✓				
Madagascar*	✓				✓			✓					
Malawi†	✓				✓				✓				
Mali	✓				✓			✓					
Mauritania	✓				✓			✓					
Mauritius	✓				✓			✓					
Morocco	✓				✓			✓					
Mozambique†	✓				✓				✓				
Namibia	✓	✓											✓
Niger	✓				✓			✓					
Nigeria†	B					✓		✓					
Rwanda*†	✓				✓			✓					
Sao Tomé and Principe	✓				✓			✓					
Senegal†	✓						✓	✓					
Seychelles*	✓				✓			✓					
Sierra Leone	✓					✓			✓				
Somalia	✓				✓				✓				
South Africa	✓				✓			✓					
South Sudan	✓				✓				✓				
Sudan	✓				✓				✓				
Tanzania†	B						✓			✓			
Togo†	✓				✓			✓					
Tunisia	✓					✓		✓					
Uganda†	B						✓	✓					
Zambia†	B						✓	✓					
Zimbabwe	✓					✓		✓					

B Using biometrics

* Countries who have expressed their intent to intoduce a data protection laws, however they have not yet entered into force
† Countries with Mobile Money regulatory changes, see page 62

ACCESS TO MOBILE SERVICES AND PROOF OF IDENTITY 2021

* Countries who have expressed their intent to intoduce a data protection laws, however they have not yet entered into force
† Countries with Mobile Money regulatory changes, see page 62

Americas

	Mandatory SIM registration	Mandatory SIM registration under consideration	SIM registration not mandated	State of SIM registration inconclusive	'Capture and Store' SIM user information	'Capture and Share' SIM user information	'Capture and Validate' SIM user information	Mandate SIM registration and have a data privacy framework	Mandate SIM registration but lack a data privacy framework	Mandate SIM registration and are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy framework
Antigua and Barbuda	✓				✓			✓					
Argentina	✓				✓			✓					
Bahamas	✓				✓			✓					
Barbados*	✓				✓			✓					
Belize	✓				✓				✓				
Bolivia	✓				✓				✓				
Brazil	✓				✓			✓					
Canada			✓										
Chile		✓										✓	
Colombia†	✓				✓			✓					
Costa Rica	✓				✓			✓					
Cuba	✓				✓				✓				
Dominica	✓				✓					✓			
Dominican Republic	✓						✓	✓					
Ecuador	✓						✓			✓			
El Salvador	✓				✓					✓			
French Guiana				✓									
Greenland				✓									
Grenada	✓				✓				✓				
Guatemala	✓				✓				✓				
Guyana	✓				✓				✓				
Haiti	✓				✓				✓				
Honduras	✓				✓					✓			
Jamaica*	✓				✓			✓					
Mexico		✓										✓	
Nicaragua			✓										
Panama	✓				✓			✓					
Paraguay	✓				✓			✓					
Peru†	B						✓	✓					
St. Kitts & Nevis*	✓				✓			✓					
St. Lucia*	✓				✓			✓					
St. Vincent and the Grenadines*	✓				✓			✓					
Suriname	✓				✓				✓				
Trinidad and Tobago	✓				✓			✓					
United States of America			✓										
Uruguay	✓				✓			✓					
Venezuela	B				✓				✓				

B Using biometrics

* Countries who have expressed their intent to intoduce a data protection laws, however they have not yet entered into force

† Countries with Mobile Money regulatory changes, see page 62

* Countries who have expressed their intent to intoduce a data protection laws, however they have not yet entered into force

† Countries with Mobile Money regulatory changes, see page 62

Asia

	Mandatory SIM registration	Mandatory SIM registration under consideration	SIM registration not mandated	State of SIM registration inconclusive	'Capture and Store' SIM user information	'Capture and Share' SIM user information	'Capture and Validate' SIM user information	Mandate SIM registration and have a data privacy framework	Mandate SIM registration but lack a data privacy framework	Mandate SIM registration and are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy framework
Afghanistan	✓				✓				✓				
Armenia	✓				✓			✓					
Azerbaijan	✓				✓			✓					
Bahrain	✓						✓	✓					
Bangladesh†	B						✓	✓					
Bhutan*	B				✓			✓					
Brunei Darussalam	✓				✓				✓				
Cambodia	✓				✓				✓				
China	B						✓			✓			
Cyprus	✓				✓			✓				✓	
Georgia	✓		✓		✓			✓					
Hong Kong		✓										✓	
India†	✓				✓					✓			
Indonesia†	✓						✓			✓			
Iran	✓				✓					✓			
Iraq	✓				✓				✓				
Isreal			✓										
Japan	✓				✓			✓					
Jordan†	✓				✓					✓			
Kazakhstan	✓				✓			✓					
Korea, North	✓				✓				✓				
Korea, South	✓				✓			✓					
Kuwait†	✓				✓				✓				
Kyrgyzstan	✓				✓			✓					
Laos	✓				✓			✓					
Lebanon	✓				✓			✓					
Macao	✓				✓			✓					
Malaysia†	✓						✓	✓					
Maldives	✓				✓				✓				
Mongolia	✓				✓				✓				
Myanmar†	✓				✓				✓				
Nepal	✓				✓			✓					
Oman	✓				✓					✓			
Pakistan†	B						✓			✓			
Palestine	✓				✓				✓				
Philippines†		✓										✓	
Qatar	✓				✓			✓					
Saudi Arabia†	B						✓		✓				
Singapore	✓				✓			✓					
Sri Lanka*†	✓				✓			✓					
Syria	✓				✓				✓				
Taiwan	✓				✓			✓					
Tajikistan	✓				✓			✓					
Thailand†	B					✓		✓					
Timor-Leste	✓				✓				✓				
Turkey	✓				✓			✓					
Turkmenistan	✓				✓			✓					
United Arab Emirates	B				✓				✓				
Uzbekistan	✓				✓			✓					
Vietnam†	✓				✓					✓			
Yemen	✓				✓				✓				

B Using biometrics

Oceania

	Mandatory SIM registration	Mandatory SIM registration under consideration	SIM registration not mandated	State of SIM registration inconclusive	'Capture and Store' SIM user information	'Capture and Share' SIM user information	'Capture and Validate' SIM user information	Mandate SIM registration and have a data privacy framework	Mandate SIM registration but lack a data privacy framework	Mandate SIM registration and are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy framework
Australia	✓				✓			✓					
Fiji†	✓				✓				✓				
Kiribati			✓										
Marshall Islands			✓										
Micronesia			✓										
Nauru			✓										
New Zealand			✓										
Palau				✓									
Papua New Guinea	✓				✓				✓				
Samoa			✓										
Solomon Islands		✓								✓			
Tonga	✓				✓				✓				
Tuvalu				✓									
Vanuatu			✓										

* Countries who have expressed their intent to intoduce a data protection laws, however they have not yet entered into force
† Countries with Mobile Money regulatory changes, see page 62

ACCESS TO MOBILE SERVICES AND PROOF OF IDENTITY 2021

* Countries who have expressed their intent to intoduce a data protection laws, however they have not yet entered into force
† Countries with Mobile Money regulatory changes, see page 62

Europe

	Mandatory SIM registration	Mandatory SIM registration under consideration	SIM registration not mandated	State of SIM registration inconclusive	'Capture and Store' SIM user information	'Capture and Share' SIM user information	'Capture and Validate' SIM user information	Mandate SIM registration and have a data privacy framework	Mandate SIM registration but lack a data privacy framework	Mandate SIM registration and are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy framework
Albania	✓						✓	✓					
Andorra	✓				✓			✓					
Austria	✓				✓			✓					
Belarus*	✓				✓			✓					
Belgium	✓				✓			✓					
Bosnia and Herzegovina			✓										
Bulgaria	✓				✓			✓					
Croatia			✓										
Czech Republic			✓										
Denmark			✓										
Estonia			✓										
Finland			✓										
France	✓				✓			✓					
Germany	✓				✓			✓					
Greece	✓				✓			✓					
Greenland				✓									
Hungary	✓						✓	✓					
Iceland			✓										
Ireland			✓										
Italy	✓					✓		✓					
Kosovo	✓				✓			✓					
Latvia			✓										
Liechtenstein			✓										
Lithuania			✓										
Luxembourg	✓				✓			✓					
Malta	✓				✓			✓					
Moldova			✓										
Monaco	✓				✓			✓					
Montenegro	✓				✓			✓					
Netherlands			✓										
North Macedonia	✓				✓			✓					
Norway	✓				✓			✓					
Poland	✓						✓	✓					
Portugal			✓										
Romania		✓										✓	
Russian Federation	✓						✓	✓					
San Marino	✓					✓		✓					
Serbia		✓										✓	
Slovakia	✓				✓			✓					
Slovenia			✓										
Spain	✓				✓			✓					
Svalbard	✓				✓			✓					
Sweden			✓										
Switzerland	✓				✓			✓					
Ukraine	✓				✓			✓					
United Kingdom			✓										

* Countries who have expressed their intent to intoduce a data protection laws, however they have not yet entered into force

* Countries who have expressed their intent to intoduce a data protection laws, however they have not yet entered into force

Mobile Money regulatory changes

	Fee Waiver	Flexible KYC and On-boarding	Social and humanitarian transfers	Increasing transaction and balance limits	Mobile money essential service declaration	Promoting digital/electronic payments	Support to agents	Others
Africa								
Burundi	✓							
Cameroon	✓							
Congo, Dem. Republic	✓		✓	✓				✓
Côte d'Ivoire	✓	✓	✓	✓				
Egypt	✓	✓		✓		✓		✓
Ethiopia				✓				
Gambia			✓					
Ghana	✓	✓	✓	✓				
Guinea	✓	✓						
Kenya	✓		✓	✓				
Lesotho	✓			✓				
Liberia	✓		✓	✓				
Malawi	✓			✓				
Mozambique	✓			✓				
Nigeria					✓			
Rwanda	✓		✓	✓				
Senegal	✓	✓	✓	✓				
Tanzania				✓				
Togo	✓	✓	✓	✓				
Uganda	✓		✓					
Zambia	✓		✓	✓				✓
Americas								
Colombia			✓					
Peru				✓				
Asia								
Bangladesh	✓		✓	✓				
India	✓					✓	✓	✓
Indonesia	✓		✓			✓		
Jordan	✓	✓						✓
Kuwait		✓						
Malaysia					✓			✓
Myanmar				✓	✓	✓		
Pakistan	✓	✓		✓		✓	✓	
Philippines	✓	✓				✓		
Saudi Arabia				✓		✓		
Sri Lanka		✓		✓	✓			
Thailand			✓					
Vietnam	✓							
Oceania								
Fiji	✓				✓			

Others = Promote interoperability, sandbox, trust account interest usage

Glossary

Head of household – The head of household is defined as someone who would typically make decisions for the household and they may also be the chief wage earner from paid work or any other form of income.

Mobile money 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).

Official form of ID – Government-recognised or government-issued ID documents which prove who you are, such as birth certificates, national ID cards, or another form of official ID.

Other form of official ID – Any other government-recognised or government-issued ID documents aside from a national ID card and a birth certificate. This may typically include a passport, a driver's licence or a voter card, among some others.

Person with disabilities – A person who reports any acute difficulty ("a lot of difficulty") or complete inability ("cannot do at all") to perform one or more of the functional domains of the Washington Group Short Set of Disability Questions.

SIM card registered in one's own name – A sub-category of 'SIM card user' (see below). When an individual presents official ID documents during mandatory SIM registration and the documents are accepted, they own a SIM card registered in their own name. This is different from using a SIM card registered in someone else's name.

SIM card user – Those that have a SIM card (i.e. mobile phone number) that they use at least once a month, in a handset that they have sole or main use of or in other people's handsets.

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.

Washington Group Short Set of Questions – A set of questions designed to identify persons with disabilities in a survey or census. Respondents answer questions and report difficulties experienced in six core functional domains: seeing, hearing, walking, cognition, self-care and communication.

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