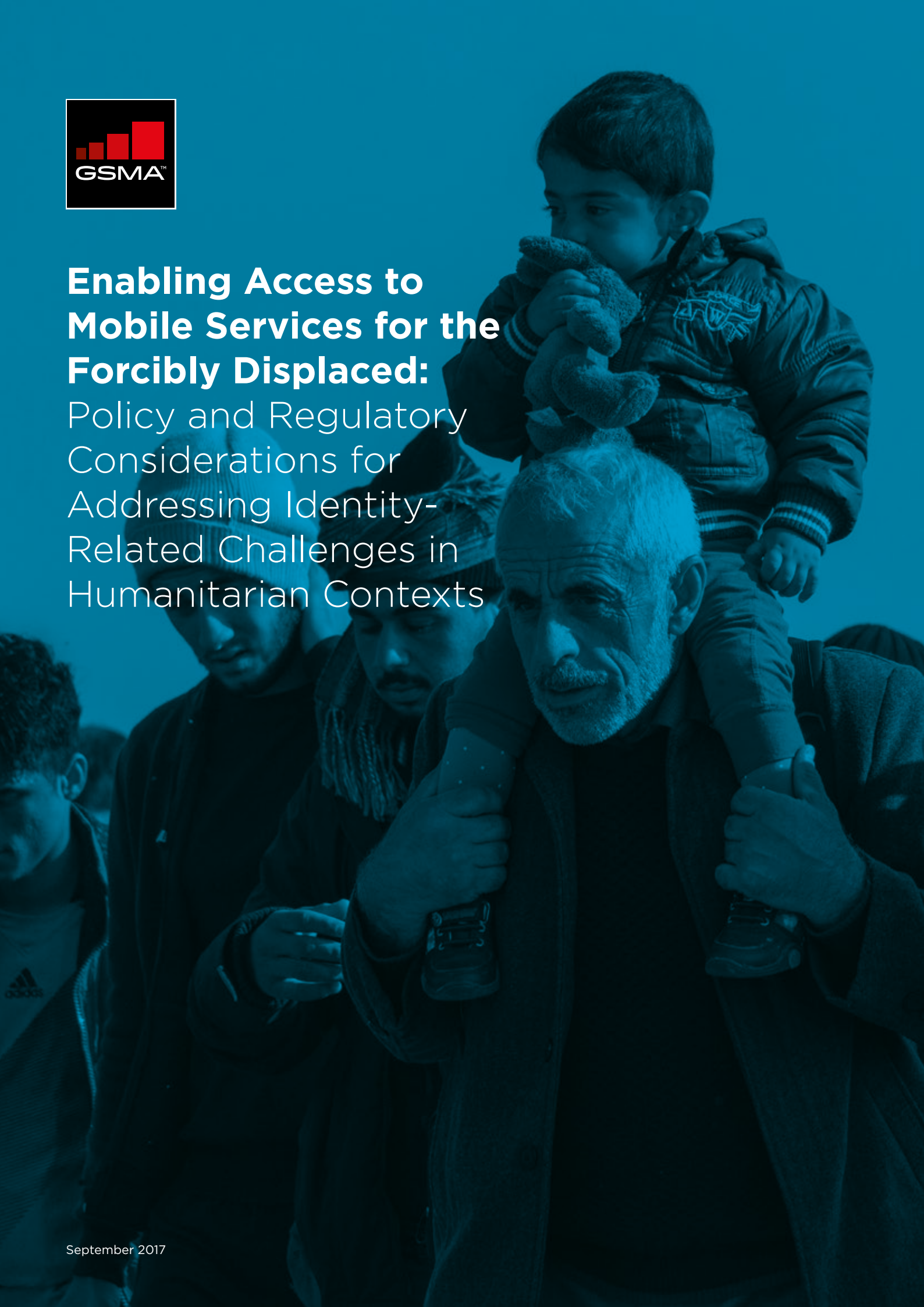

Enabling Access to Mobile Services for the Forcibly Displaced:

Policy and Regulatory Considerations for Addressing Identity-Related Challenges in Humanitarian Contexts

September 2017

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 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 industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of 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

Mobile Money

The GSMA's Mobile Money programme works to accelerate the development of the mobile money ecosystem for the underserved.

For more information, please visit the GSMA Mobile Money website at www.gsma.com/mobilemoney or email us as mobilemoney@gsma.com

Follow GSMA Mobile Money on Twitter: @GSMAmmu

Acknowledgements
The GSMA is grateful to the interviewees and peer reviewers of this report, notably: from the Office of the United Nations High Commissioner for Refugees (UNHCR), with special thanks to reviewers from their Cash Based Interventions Unit, the Identity Management Unit, the Data Protection Unit and the Innovation service; the World Food Programme (WFP), the United Nations Capital Development Fund (UNCDF); the International Rescue Committee (IRC); the Consultative Group to Assist the Poor (CGAP); the Alliance for Financial Inclusion (AFI); and Mercy Corps.

Contents

Context and scope of this Policy Note

The importance of mobile phones, networks and services to people's lives today is undisputed. However, the increasing emphasis on proof-of-identity requirements is preventing large numbers of underserved people who lack identification documents to access mobile services. There are a number of other factors preventing people from accessing mobile services, such as limited network connectivity or low levels of digital literacy. In this Policy Note, we focus on identity-related barriers preventing Forcibly Displaced Persons (FDPs), including refugees, from accessing mobile connectivity and mobile financial services (MFS). This Note offers several considerations for host-country governments and regulators on how to potentially address such barriers, being mindful that the responsibility for issuing identification credentials to FDPs is usually born by different entities depending on the circumstances relating to a person's forced displacement status (e.g. whether someone is an asylum seeker, refugee, stateless person, internally displaced person etc.) Finally, the Note outlines several benefits to host countries, local communities and the humanitarian aid sector, where mobile services – including mobile money accounts – are readily accessible by FDPs.

Summary of recommended considerations for policymakers

In an effort to promote an enabling policy and regulatory framework, host-country governments and regulators (including central banks) should consider adopting flexible and proportionate approaches towards proof-of-identity requirements for forcibly displaced persons to be able to access mobile services, particularly in emergency contexts. Such approaches may include:

1. Providing clear guidelines on what identification is acceptable for FDPs to access mobile services, and ensuring that a critical mass of FDPs has access to an acceptable form of identity;
2. Allowing the use of UNHCR-issued identification, where available, to satisfy any mandatory SIM registration or 'Know Your Customer' (KYC) requirements for opening mobile money accounts;
3. Enabling lower, 'tiered' thresholds of KYC requirements to allow FDPs to open basic mobile money accounts, particularly in emergency contexts;
4. Harmonising identity-related SIM registration requirements with the lowest-tier of KYC requirements in countries where SIM registration is mandatory;
5. Establishing proportionate Risk Assessment processes that take into account the diverse types of FDPs when considering proof-of-identity policies;
6. Exploring the use of new Digital Identity technologies;
7. Promoting robust identity validation processes while adopting consistent data protection and privacy frameworks.

Introduction

The ability to prove one's identity is essential to securing access to a number of life-enhancing services such as healthcare, education, financial services, connectivity and social protections[1]. Yet, an estimated 1.1 billion people[2] lack formal identification, predominantly in developing countries across Sub-Saharan Africa and Asia. For the public sector, the identity gap creates challenges around implementing and measuring social engagement and upholding civil rights such as voting, healthcare, employment, economic participation and education.

Lack of identification is also a key barrier to accessing basic mobile services – such as voice communications and messaging – in over 135 countries where proof-of-identity is mandatory to register a mobile SIM[3]. Furthermore, in order to open a mobile money account, people need to meet 'Know Your Customer' (KYC) requirements, which typically require the presentation of a formal proof-of-identity. Twenty per cent of adults cite a lack of identification as a key barrier to financial inclusion[4].

The situation is much exacerbated for forcibly displaced persons (FDPs)[5]. The United Nations High Commissioner for Refugees (UNHCR) estimates that more than 65 million people are forcibly displaced worldwide[6], many of whom have been forcibly displaced for over two decades[7]. An additional 25.4 million people are displaced every year due to natural disasters and climate-related events[8]. FDPs often relocate within their own countries or to other countries without any form of legal identification as these may have been forgotten, lost, destroyed or stolen during their journey, while those who are fleeing persecution based on some aspect of their identity (e.g. nationality, religion, ethnic group, sexual orientation, membership of a particular social group or political affiliation etc.) may decide not to travel with documentation[9].

The top ten refugee hosting countries in terms of volume have mandatory SIM registration policies in place[10] in addition to KYC identity compliance requirements for opening mobile money accounts. Many FDPs are therefore unable – at least in the short term – to meet these requirements and risk being excluded from using mobile and Mobile Financial Services (MFS). The Alliance for Financial Inclusion (AFI) recently found[11] that the main regulatory challenge identified by its members (central banks and financial regulators), without exception, was determining acceptable identification and risk management procedures for FDPs.

1. See UN's Sustainable Development Goals (SDGs) 1,3,4 and 16.9 at https://sustainabledevelopment.un.org/?menu=1300
2. World Bank ID4D initiative: http://www.worldbank.org/en/programs/id4d
3. GSMA report: Mandatory Registration of Prepaid SIM cards: https://www.gsma.com/publicpolicy/mandatory-registration-prepaid-sim-cards
4. World Bank: http://pubdocs.worldbank.org/en/113791483565360488/N2UnbankedV5.pdf
5. For the purposes of this note, the term 'FDPs' includes refugees, internally displaced persons (IDPs) e.g. those fleeing a war zone and/or relocating in the aftermath of a natural disaster, asylum seekers and other persons who have had to leave their homes as a result of a natural, technological or deliberate event. (Definition adapted from http://iasfm.org/)
6. UNHCR: http://www.unhcr.org/uk/figures-at-a-glance.html
7. UNHCR: Global Trends, http://www.unhcr.org/576408cd7.pdf
8. CGAP/World Bank report: The role of financial services in humanitarian crises - http://www.cgap.org/publications/role-financial-services-humanitarian-crises
9. GSMA report: Refugees and Identity: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/06/Refugees-and-Identity.pdf
10. GSMA report: Mobile Money, Humanitarian Cash Transfers and Displaced Populations': https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/05/Mobile_Money_Humanitarian_Cash_Transfers.pdf
11. AFI report: http://www.afi-global.org/sites/default/files/publications/2017-07/AFI_displaced%20persons_AW_digital.pdf

Positive outcomes created by enabling mobile access for FDPs

Enabling access to mobile services can lead to positive outcomes not just for FDPs themselves but also for humanitarian agencies, host-governments and local communities. For example:

1 Benefits for FDPs

- **Ability to communicate with loved ones.** Mobile phones can help displaced persons re-connect or re-unite with lost family members and friends, as well as enabling access digital and educational services[12].

- **Financial inclusion.** Mobile money has already been game-changing for hundreds of millions of underserved people who are now safer, more productive with their time and their money, and able to take advantage of increased socio-economic opportunities[13]. In the case of FDPs, mobile money can act as a gateway to financial inclusion, which is particularly critical for refugees considering that 80% of refugee crises last for ten years or more[14].

- **A convenient way of receiving financial aid and remittances from family and friends anywhere and at any time.** This flexibility can make life easier for those based in hard-to-reach areas. The density and reach of mobile money distribution networks also means that, when one does need to interact with an agent, that agent is likely to be relatively close. Mobile-enabled humanitarian assistance may also provide a more dignified experience to beneficiaries by giving them a greater choice and autonomy to determine what their needs are and how to meet them and fostering feelings of inclusivity.

- **Empowerment and improved livelihoods and productivity.** Mobile access and mobile money services give FDPs access to information, capital (through remittances), payment solutions, and potential revenue streams, which are critical building blocks for the productivity of these communities[15]. For example with mobile money, FDPs can monitor and retain a clear record on their phone of what has been sent. They can in turn use this information to access other types of services and economic opportunities.

12. GSMA report: The Importance of Mobile for Refugees: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/02/The-Importance-of-mobile-for-refugees_a-landscape-of-new-services-and-approaches.pdf
13. In 2016, there were over half a billion mobile money accounts globally and more than 40 per cent of the adult population were actively using mobile money in eight countries: Gabon, Ghana, Kenya, Namibia, Paraguay, Tanzania, Uganda, and Zimbabwe. GSMA report: State of the Industry Report on Mobile Money: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/GSMA_State-of-the-Industry-Report-on-Mobile-Money_2016-1.pdf
14. HPG Commissioned Report: Protracted displacement: uncertain paths to self-reliance in exile: https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9851.pdf
15. GSMA report, Disaster Response – Mobile is a Lifeline: Research from Nyarugusu Refugee Camp, Tanzania - https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/07/mobile-is-a-life-line.pdf

2 Benefits for host-country governments and local communities

- **Reduced reliance on state resources.** There is growing recognition that FDPs may become 'aid dependent'[16] unless they have the option to achieve financial independence. By offering them opportunities to securely store money, save and make/receive payments, access to mobile financial services may[17] therefore assist FDPs in becoming increasingly self-reliant, reducing their vulnerability and long-term dependence on humanitarian or external assistance. FDPs who can build and protect their livelihood assets are also more able to return to their home countries when it is safe to do so[18].

- **Reduced risks of financial exclusion and strengthened financial integrity.** Enabling FDPs to access mobile financial services is critical to allow them to participate in a formal financial system systematically. Reducing the risks of financial exclusion is also vital to achieving an effective anti-money laundering system and countering the financing of terrorism (collectively known as AML/CFT system). Enabling FDPs to access MFS is therefore critical to help regulators and governments achieve both financial inclusion and financial integrity objectives[19].

- **Increased economic activity in local host communities.** Host communities (whether urban, rural or those near refugee camps) can benefit as new markets are created for local producers and other enterprises. For example, FDPs could redeem their humanitarian aid food vouchers or buy food using their mobile money credit to the benefit of local farmers, food producers and retailers. It is also common[20] for marketplaces to operate near or at the entrance of refugee camps where both refugees and host communities are permitted to trade. Local mobile money agents will also benefit from this increased economic activity e.g. through commissions from cash-out transactions. Mobile can therefore contribute to the promotion of social cohesion between FDPs and local communities.

16. AFI report – see footnote 28, above
17. This may be dependent on contextual factors, for example on whether the mobile money account is considered a de facto bank account or if it's a virtual account under agency control. The latter has implications regarding ownership of funds until the funds have been withdrawn, which has an impact on whether the account can be used for saving and what happens when agency funds are merged with personal funds.
18. UNHCR report: Promoting Livelihoods and Self-reliance - http://www.unhcr.org/uk/publications/operations/4eeb19f49/promoting-livelihoods-self-reliance-operational-guidance-refugee-protection.html
19. Financial Action Task Force (FATF) (2012), "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation". Available at http://www.fatf-gafi.org
20. http://documents.wfp.org/stellent/groups/public/documents/ena/wfp286682.pdf
21. Ibid
22. GSMA report: Mobile Money, Humanitarian Cash Transfers and Displaced Populations': https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/05/Mobile_Money_Humanitarian_Cash_Transfers.pdf
23. Source: http://www.unhcr.org/581363414.pdf

3 Benefits for humanitarian agencies

Innovations in technology have brought about a shift in the way humanitarian agencies have been leveraging the mobile platform to deliver aid to FDPs, communicate with them and improve their own operational processes[21]:

- **Ability to scale up humanitarian response through mobile-enabled cash transfers and mobile vouchers.** Cash transfers are increasingly used as a mechanism for delivering aid[22] and digital payments are often cited as one of the key developments, which enables humanitarian action to increase its reach. Other benefits include improved accountability, security, as well as faster, more transparent and traceable aid disbursement. Humanitarian agencies can also benefit from the cost effectiveness and scalability of using mobile technology to deliver aid. Of note, is the UNHCR's stated goal[23] that by year 2020, its "operations will, wherever feasible, use direct transfer arrangements for delivering cash assistance to refugees and other persons of concern [...] through digital means such as bank cards and mobile money". The UN's largest humanitarian agency, the World Food Programme (WFP) has supported more than 14 million people globally to access food. This is often achieved through mobile money cash transfers and mobile food vouchers[24] that are redeemable at specific predefined locations (such as local food merchants). These vouchers are typically based on SIM cards with restricted functionalities that tend to be exempt from registration requirements or that are registered under the humanitarian agency's name. While these closed-loop systems have proved to be successful in addressing a vital social need in specific contexts and can lead to operational efficiencies[25], the beneficiaries' inability to use the mobile SIM for any form of communication or for opening a mobile money account may create a missed opportunity for them to be digitally, socially and financially included.

- **Improved communications with FDPs:** Where FDPs have access to active mobile SIMs, humanitarian organisations are increasingly utilising mobile platforms to communicate with them via SMS[26]. UNHCR, in conjunction with national governments and local authorities, aim to continuously validate refugees' records to better protect and help them find a durable solution (i.e. voluntarily return home, integrate into the local country, or settle in a third country). This requires UNHCR and/or the host government to be in regular contact with refugees who, from time to time, may be asked to check in with UNHCR to either provide or receive new information. To better achieve these objectives, it would be ideal for as many FDPs as possible to able to access a mobile SIM but also for governments and humanitarian agencies to develop relevant, life-enhancing services accessible through mobile, so that FDPs have tangible incentives to maintain an active SIM.

Many actors, including AFI[30] , the Bill and Melinda Gates Foundation[31], CGAP[32], the International Rescue Committee[33], Mercy Corps[34], the UNHCR[35], the World Economic Forum[36] and the WFP[37] are advocating for stronger public-private partnerships to address identity and mobile connectivity challenges to better utilise the mobile platform for delivering aid to FDPs.

24. Such as the Bamba Chakula Initiative in Kenya led by the WFP and Safaricom.
25. Preliminary findings by the World Food Programme showed the introduction of electronic food vouchers in two camps in Kenya increased cost-effectiveness by 11% (cheaper than delivering in-kind food assistance). See: http://iati.dfid.gov.uk/iati_documents/5497926.odt
26. Humanitarian organisations can use SMS to ask FDPs to update or verify their personal details, maintain dialogue and monitor the capacity of designated accommodation areas. A 2014 SMS exercise led by UNHCR, for instance, helped reveal that 15,000 fewer refugees remained in the Za'atari camp in Jordan than UNHCR had been estimating; https://saltimpact.com/leveraging-social-media-sms-technology-communicate-refugees-zaatari-camp/
27. See UNHCR's Handbook for Registration: http://www.refworld.org/pdfid/3f967dc14.pdf
28. In Kenya for example, months can pass by between a refugee's initial registration and their interviews with government authorities – access to a mobile phone can support a reminder being sent to the refugee with the date/time of their interview and limit costs and delays associated with non-attendance. See: https://kanere.org/2009/02/28/refugee-status-determination-justice-delayed-istypical/
29. Anecdotal evidence suggests that refugees may discard SIM cards issued by humanitarian agencies if they fear deportation or discrimination by host-country governments.
30. http://www.afi-global.org/sites/default/files/publications/2017-07/AFI_displaced%20persons_AW_digital.pdf
31. http://www.cashlearning.org/downloads/enabling-digital-financial-services-in-humanitarian-response-four-priorities-for-improving-payments.pdf
32. http://www.cgap.org/sites/default/files/Forum-The-Role-of-Financial-Services-in-Humanitarian-Crises_1.pdf
33. https://www.rescue-uk.org/outcome/cash-relief
34. https://www.mercycorps.org/sites/default/files/Financial%20Inclusion%20Capacity%20Statement%20-%202017.pdf
35. http://www.unhcr.org/5770d43c4.pdf
36. https://www.weforum.org/reports/the-future-of-humanitarian-response-2017
37. https://www.wfp.org/world-humanitarian-summit/empowerment-through-cash-transfers

Factors exacerbating proof-of-identity challenges for FDPs

Realising these outcomes described above is highly predicated on whether the affected populations can meet the host-countries' identification requirements to register for a SIM card or open a mobile money account. A number of factors may exacerbate proof-of-identity challenges for FDPs:

(a) Inconsistent approaches for issuing identification credentials and ambiguity on how to meet SIM registration and KYC requirements

In practice, the process through which FDPs are registered and issued identity documents, and their ability to use these documents to gain access to different types of services is extremely contextual and can vary significantly by country and the circumstances that led to the forced displacement[38]. For example, host-country governments are generally responsible for the registration of internally displaced persons[39]. In the case of refugees or asylum seekers who have crossed borders, registration usually involves a joint effort between the host government and UNHCR, with the latter playing a greater role in the registration processes where host-country governments lack the capacity or willingness to do so. Although it is ultimately the responsibility of the State to register refugees and issue identification documents[40], UNHCR has a mandate to provide support and assistance where necessary in order to ensure these functions are carried out according to international standards[41]. However, identification documents issued by UNHCR and other humanitarian agencies may or may not be accepted to register a mobile SIM or as a form of KYC to open a mobile money account. This can be because such documents are not legally recognised by the relevant authorities or because their function is confined to attestation of refugee status or their entitlement to assistance.

Furthermore, most host-countries where proof-of-identity is mandated for mobile SIM registration or for opening mobile money accounts, have not adapted their lists of acceptable identification documents with flexibility to cater for FDPs in times of crisis. For example, regulations may only allow for host-country government-issued identification documents to be used[42], which FDPs may face delays and challenges in obtaining. The situation could be worse in emergency contexts such as the aftermath of a natural disaster. The strict enforcement of KYC rules can create challenges for humanitarian organisations and mobile operators[43] resulting in unrealistic expectations for disbursing cash to beneficiaries. Similarly, rules that are too vague and ambiguous may lead to mobile operators within the same region interpreting them differently and requiring FDPs to present varying types of identification.

38. GSMA report: Refugees and Identity - https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/06/Refugees-and-Identity.pdf
39. http://www.ohchr.org/EN/Issues/IDPersons/Pages/Issues.aspx
40. See Articles 27 and 28 of the 1951 Refugee Convention: http://www.unhcr.org/uk/1951-refugee-convention.html
41. http://www.unhcr.org/526a22cb6.pdf
42. Ibid- For example, in Kenya, refugees need to obtain an alien card from the National Registration Bureau in order to register for a SIM card or open a mobile money account. The typical waiting period for this is about three years, and in some cases this process has taken as long as seven years. See GSMA's 'Refugees and Identity' report and https://kanere.org/2009/02/28/refugee-status-determination-justice-delayed-istypical/
43. AFI report – see footnote 28, above

(b) Lack of proportionate risk-management frameworks to cater for FDPs' unique circumstances

Mobile money providers have to comply with local AML and CFT regulations. According to the Financial Action Task Force (FATF)[44], the implementation and enforcement of such rules needs to be proportionate and risk-based. The risks associated with the use of mobile money by FDPs as well as their financial needs will vary depending on their circumstances (e.g. whether they are in transit or living in more stable environments, their legal and financial status, age, education, financial and technical literacy, country of origin, etc.[45]). Customer due diligence requirements (CDD) should therefore cater for the differences in risk-profiles. In a simplified scenario where for example a host-government imposes a blanket policy that all FDPs are classed as 'high risk' for AML/CFT purposes, many people would be unable to meet the KYC requirements for opening mobile money accounts. The risks of digital and financial exclusion for FDPs are therefore higher in countries where risk-based and proportionate KYC frameworks are not in place.

(c) Lack of interoperability among registration systems

While UNHCR has the official mandate to register refugees jointly with the Government, a number of other humanitarian agencies, including the WFP and the International Committee of the Red Cross (ICRC) account for different groups of FDPs using distinct processes, and issue functional – and increasingly biometric[46] – identification credentials, which are recorded and stored in databases that each organisation manages separately. For many refugees, a UNHCR-issued registration document is the only identification that they may have access to. While there is on-going collaboration[47] between humanitarian agencies to harmonise beneficiary databases, the general lack of interoperability and standardisation across the various systems may lead to a reluctance by certain host-country governments to coordinate with the various actors or allow the use of these identification documents to register a SIM or open a mobile money account.

44. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf
45. Furthermore, certain refugee groups may face a higher risk of persecution-related vulnerabilities while the legal protections available to them might vary according to the policies of the host country they had sought refuge in. Such risks could materialise if, for example, host-countries conduct background checks involving contact with authorities from a refugee's country of origin.
46. See UNHCR's BIMS system at http://www.unhcr.org/uk/protection/basic/550c304c9/biometric-identity-management-system.html and the WFP's ' SCOPE platform: http://documents.wfp.org/stellent/groups/public/documents/resources/wfp280992.pdf
47. The UN's Common Treasury Services unit is focusing efforts on promoting cash collaboration, coordination, harmonisation and digitisation across UNHCR, WFP, and UNICEF.

Policy and regulatory considerations for addressing proof-of-identity challenges for FDPs

The potential benefits of enabling FDPs to access mobile services outlined above underscore the need for humanitarian agencies, host-country governments, regulators, mobile operators and MFS providers to collaborate on solutions that can enable more FDPs to overcome identity-related barriers that prevent them from accessing mobile services[48]. In order to facilitate access to mobile connectivity and mobile money services, host-country governments, telecoms and financial sector regulators should consider the following recommendations:

1. Providing clear guidelines on what identification is acceptable for FDPs to access mobile services, and ensuring that a critical mass of FDPs has access to an acceptable form of identity. Where mobile SIM registration and/or KYC processes for mobile money accounts are mandated, host-country governments should ensure that the list of acceptable identification documents is publicly available, clear and unambiguous and that a critical mass of FDPs has had the opportunity to access an acceptable form of identity. When new mandatory SIM registration requirements are established, governments should also allow adequate time for FDPs to register their SIM cards before requesting mobile operators to disconnect existing users who don't meet the new requirements. Where it is in the host-country governments' purview to issue identification (for example to IDPs), policymakers may also consider leveraging national identification systems where they exist to provide FDPs with an acceptable form of identification[49] if relevant and proportionate in a given context.

2. Allowing the use UNHCR-issued identification, where available, to satisfy any mandatory SIM registration / KYC for mobile money. As part of their mandate, the UNHCR issues identification[50] for refugees, as well as proof of registration for asylum seekers in conjunction with host-country governments. In the context of such collaboration, the identification or registration credentials issued to refugees and asylum seekers could be designed to reflect the local context, standards and processes expected by the host-country government. Policymakers should therefore consider allowing refugees and asylum seekers to use such identification credentials for meeting mobile SIM registration or KYC requirements. This approach was followed in a number of countries, including Jordan and Egypt[51]. As a result, humanitarian organisations have been able to reach beneficiaries directly, improving transparency, expediency and operational efficiency of the funds' disbursement process. However, this approach by itself may not always be helpful in the case of FDPs who have not obtained UN Identities – for example internally displaced persons or FDPs living outside refugee camps – or who choose not to officially register if they fear deportation or detention.

48. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/06/Refugees-and-Identity.pdf
49. This approach may however not be appropriate in contexts where a government is potentially part of the reason why certain IDP groups were internally displaced.
50. http://www.unhcr.org/afr/who-we-help.html
51. See for examples approaches in Jordan, Iraq, Afghanistan, Egypt, Rwanda, Pakistan, the Philippines and Haiti referenced in the various GSMA reports mentioned in this note

3. Enabling lower, 'tiered' thresholds of KYC requirements for the opening of mobile money accounts by FDPs, particularly in emergency contexts.

In a few countries such as Iraq, the Central Bank has granted an exception that allows refugees on UNHCR's biometric database to meet a lower threshold of KYC requirements to open entry-level mobile money accounts with limited functionalities, simply by presenting their UNHCR registration certificate to a mobile money agent. In Haiti, the regulator allowed the creation of a limited 'mini-wallet' with reduced KYC requirements to enable humanitarian cash assistance via a mobile money account to individuals impacted by the 2010 earthquake[52]. Similarly in the Philippines, following Typhoon Haiyan, the Central Bank[53] temporarily relaxed the KYC rules (after the Government declared a 'State of Calamity') to allow those who had been displaced and lost all forms of ID to still access mobile money services.[54] All insurance companies also temporarily relaxed KYC requirements to allow the claims to be processed immediately. Such flexibility in the enforcement of identity requirements is welcome, and policymakers should seek to ensure that their policies are clear and unambiguous – including how they may vary in different contexts – to ensure regulatory certainty and limit different interpretations by humanitarian agencies, the various mobile operators and other mobile money providers.

4. Harmonising identity-related SIM registration requirements with the lowest-tier of KYC requirements in countries where SIM registration is mandatory.

In countries that have adopted a proportionate tier-based approach to KYC for mobile money, like Sri Lanka, KYC requirements do not generally exceed the SIM registration requirements. Where policymakers decide to impose proof-of-identity requirements for mobile SIM registration, they should seek to harmonise these with the lowest KYC threshold requirements,[55] if relevant. Taking an integrated policy approach to these requirements would simplify the end-user journey and enable FDPs to also open a mobile money account at the point of SIM registration. This will require close collaboration between the telecommunications regulator or the relevant Ministry dealing with SIM registration rules and the financial sector regulator dealing with KYC requirements.

5. Establishing proportionate Risk Assessment processes that take into account the diverse types of FDPs when considering proof-of-identity policies.

As highlighted earlier, the risks associated with the use of mobile money services by FDPs are likely to vary given the diversity of FDPs' circumstances. It is therefore important for policymakers to develop Risk Assessment processes that take into account these factors when introducing or enforcing proof-of-identity requirements. This should help ensure that the lower-risk and more vulnerable FDPs are not inadvertently excluded from accessing mobile services. The Financial Action Task Force (FATF)[56] has provided helpful recommendations in relation to the steps financial service providers could undertake to comply with CDD. FATF also urges policymakers to apply a risk-based approach when applying these measures to cater for certain vulnerable groups so as not to unreasonably exclude them from accessing financial services (including mobile money). If for example a FDP is assessed as a low income / low risk for money laundering or terrorist financing, 'simplified due diligence' measures should be adopted[57]. This could include obtaining less information about the customer's identity or postponing the identity verification for a specified time period that would reasonably allow that customer to obtain an acceptable proof-of-identity (from the host-government or a humanitarian organisation). In considering these factors, financial sector and telecoms regulators should work closely together to provide guidance on how mobile money providers should conduct customer identification

52. http://odihpn.org/magazine/innovation-in-emergencies-the-launch-of-%C2%91mobile-money%C2%92-in-haiti/
53. See: UNOCHA/UNICEF report: Cash Transfer Programming: The Haitian Experience, accessed at: https://www.humanitarianresponse.info/system/files/documents/files/ctp_the_haiyan_experience_june_2015_draft_fullreport.pdf
54. GSMA report: Disaster Response – Mobile Money for the Displaced: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/01/Disaster-Response-Mobile-Money-for-the-Displaced.pdf
55. See GSMA report: Regulatory and policy trends impacting Digital Identity and the role of mobile Considerations for emerging markets: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/10/Regulatory-and-policy-trends-impacting-Digital-Identity-and-the-role-of-mobile.pdf
56. The FATF Recommendations: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf
57. See FATF, October 2014, "Guidance for a Risk-Based Approach: The Banking Sector". Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf

and verification for FDPs in practice. Finally, there is always a trade-off to be considered between the utility of an identity verification system and the risks it presents. In assessing such trade-offs, policymakers should carefully balance the benefits arising from FDPs' access to mobile services against the risk of excluding them on the basis of non-compliance with identification requirements.

6. Exploring the use of new Digital Identity technologies. Recent initiatives have shown that new technologies – such as distributed ledgers, digital identity/attribute verification solutions etc. – can help FDPs establish functional identities, often linked to biometrics but with data protection and privacy mechanisms built in. For example, through their 'Building Blocks'[58] initiative, the World Food Program (WFP) has leveraged Blockchain to make their cash-based transfer operations faster, cheaper and more secure. In Jordan[59], Building Blocks uses a smartphone interface to allow WFP personnel to authenticate and record the transactions made when vulnerable families received their food or cash assistance. This ensures that disbursements are reaching the intended beneficiaries, and also helps WFP track and verify how families are using these funds. WFP has a system that relies on biometric registration data from UNHCR[60], and uses biometric technology for authentication purposes; refugees purchase food from local supermarkets in the camp by having their iris scanned at the point of sale, instead of cash, vouchers or e-cards. Mobile operators are also well placed to play a role in the development of a digital identity ecosystem and help governments leapfrog traditional paper-based ID systems. They can achieve this by leveraging the reach of the mobile platform, their extensive network of agents, access to unique customer attributes, experience in building customer relationships and ability to comply with local laws given they are locally licensed[61]. Mobile operators may also provide credentials and authentication solutions[62] as digital identity-enabled services become more widely available. Host-country governments can support and encourage such efforts through collaborations with both the humanitarian and private sectors.

7. Promoting robust identity validation processes while adopting consistent data protection and privacy frameworks. Experience from a number of mobile operators around the world[63] who are required to comply with SIM registration/KYC processes, suggests that the verification of identity credentials can be faster and more robust where operators are able to query government databases in real time. While only a few governments have enabled mobile operators to use such real-time ID verification systems, the process usually involves the generation of a positive or a negative response to a query by a mobile operator e.g. confirming that the name and the identification credentials presented by an individual at the point of registration form a match. However, as registration and validation processes involve the handling of mobile users' personal data, the creation of policy, legal and technical frameworks that respect their privacy and set out data protection standards is crucial to building trust in any identification system. This is also a well articulated principle in the World Bank led 'Principles on Identification for Sustainable Development'[64] (endorsed by the GSMA), the World Economic Forum's 'Principles on Public Private Cooperation in Humanitarian Payments'[65], the 'Barcelona Principles for Digital Payments in Humanitarian Response'[66], UNHCR's Data Protection Policy[67], WFP's Guide to Personal Data Protection and Privacy[68] and others.

Finally, increasing reports of government requests to access communications pose a risk to consumers' trust and perceptions of identity solutions. Regulators and policymakers need to promote transparency and proper lawful management of such government access requests, to engender trust in identity-linked mobile services.

58. https://www.wfp.org/news/news-release/blockchain-against-hunger-harnessing-technology-support-syrian-refugees
59. The WFP disbursed over $1m USD through 100,000 transactions to over 10,500 beneficiaries in Jordan See: Hila Cohen's presentation at https://unite.un.org/techevents/blockchain
60. UNHCR has also deployed a Global Distribution Tool, which allows biometric verification (using iris or fingerprints) against their Biometric Identity Management System (BIMS) See: http://www.unhcr.org/550c304c9.pdf
61. See the GSMA's Digital Identity Programme: https://www.gsma.com/mobilefordevelopment/programmes/digital-identity
62. For example, Mobile Connect: https://www.gsma.com/identity/mobile-connect
63. GSMA reports: Mandatory Registration of Prepaid SIM cards: https://www.gsma.com/publicpolicy/mandatory-registration-prepaid-sim-cards
64. https://www.gsma.com/identity/wp-content/uploads/2017/02/Identification-Principles.pdf
65. http://www3.weforum.org/docs/IP/2016/FS/WEF_FI_Principles_Humanitarian_Payments.pdf
66. https://static.globalinnovationexchange.org/s3fs-public/asset/document/Digital-Payments-Humanitarian-Principles_0.pdf?BvMH5s_7H6psd5btsC7ZIS3v8KBx4Xdj
67. http://www.refworld.org/docid/55643c1d4.html
68. https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/

Conclusion

It is clear that mobile services, including connectivity and mobile money, are playing an increasingly significant role in the delivery of humanitarian assistance. While the reach of mobile networks and phones grows, so does the number of forcibly displaced persons as well as the need and opportunity for humanitarian aid agencies to support them by leveraging the mobile platform. Host-country governments have a key role to play in facilitating FDPs' access to identification, but also in deciding what identity requirements are needed for FDPs to access mobile services. Ensuring an enabling and proportional policy and regulatory environment and promoting dialogue between key stakeholders including mobile operators, MFS providers, donors, humanitarian agencies, NGOs, central banks and policymakers will be crucial to accelerating the delivery of digital humanitarian assistance.

gsma.com

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