CONNECTIVITY FOR REFUGEES

DISPLACED & DISCONNECTED



UNHCR
The UN Refugee Agency

CONNECTIVITY FOR REFUGEES

DISPLACED & DISCONNECTED

Made possible thanks to
the generous support of:

LUXEMBOURG
AID & DEVELOPMENT

UNHCR
Innovation
Service

UNHCR
The UN Refugee Agency

In partnership with:



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

For more information, please visit the GSMA corporate website at www.gsma.com
Follow the GSMA on Twitter: @GSMA

An evidence base is strongly needed to inform appropriate action. This report therefore focuses on a relatively under-explored, but nonetheless significant barrier to access among refugees and other displaced persons: legal and regulatory requirements mandating that an individual's ID is authenticated before accessing a mobile connection, bank account or mobile money wallet. This research is the first of its kind to systematically understand and address the combination of these challenges.

TABLE OF CONTENTS

Executive Summary 1
Acknowledgments 2
Abbreviations 3
1. Introduction 5
    Populations of Concern 6
    Research Questions 7
    Structure of Report 7
    Intended Audience 8
2. Humanitarian Context: Why Connectivity, Financial Services, and ID Matter 9
    Value of Connectivity for Displaced Persons 9
    Financial Inclusion and Displacement 11
    ID as an Enabling ‘Golden Thread’ 12
3. Policy Background: ID Mandates 15
    Evolution of SIM Registration Requirements 15
    Globalization of ID Requirements for Financial Services 17
4. Analysis 19
    Access to ID Credentials 19
    Access to SIM Cards 23
    Access to Bank Accounts 25
    Access to Mobile Money 27
5. Findings 29
    ID-related Access Barriers Remain 29
    Formal Workarounds Can Be Effective, Where Appropriate 29
    Informal Workarounds Are Common, But Precarious and Unsustainable 29
    Strict Requirements Risk Further Marginalizing the Vulnerable 29
    Tiered KYC/CDD Requirements Can Increase Access 30
    Broadening Access to Government-Recognized ID is Key 30
    Legal Certainty Enables Efficient Programming 31
    Policy Change is Possible, Often through Joint Advocacy 31
    More than Advocacy is Needed 31
6. Recommendations 32
    Recommendations for Government Agencies and Regulatory Bodies 32
        Clarify Existing Requirements 32
        Coordinate Across Government and with Humanitarian Partners 32
        Issue ID Credentials More Expeditiously 32
        Consider Including the Displaced in Foundational ID Platforms 33
        Assist Authentication 33
        Implement Tiered ID Requirements 33
        Harmonize ID Requirements 33
        Better Manage Policy Change 34
        Explore Regulatory Sandboxes 34
    Recommendations for UNHCR and Other Organizations 34
        Promote Good Practices Globally 34
        Facilitate Faster Registration/Documentation 35
        Monitor Government ID Issuance and Policy Change 35
        Explore eKYC Mechanisms 35
        Protect Data 36
        Encourage Service Providers to Become 'Refugee Ready' 36
7. Final Thoughts 37
    Emerging Issues 37
    Future Research 38
References 41

Executive Summary

UNHCR recognizes that one of the 'hard stops' in facilitating mobile connectivity and access to finance for displaced populations is non-conducive regulatory environments. In particular, ID-related legal requirements have proven a significant barrier to access. For example, a refugee who cannot legally activate a mobile connection, open a bank account or access a mobile money wallet in his or her own name may be further marginalized and disempowered as access to information, communication, cash assistance, and transfers is severely limited. Moreover, the lack of legal certainty, inconsistently applied regulations or sudden changes in regulatory expectations as regards identification can disrupt the delivery of humanitarian assistance.

As such, UNHCR undertook research in partnership with the GSM Association (GSMA) in the latter half of 2018 to examine these access barriers across 20 priority countries: Afghanistan, Bangladesh, Brazil, Burundi, Cameroon, Central African Republic, Chad, Democratic Republic of Congo, Ethiopia, Jordan, Kenya, Lebanon, Mauritania, Niger, Nigeria, Rwanda, Tanzania, Turkey, Uganda, and Zambia. The results of the study demonstrate that:

- In a majority of countries, displaced persons continue to face legal barriers to accessing SIM cards and opening bank and mobile money accounts in their own name. Many of the issues relate to proof-of-identity documentation for the displaced. There are both policy issues at play (i.e. government positions to restrict access to ID credentials), as well as operational concerns (e.g. the time it takes for governments to issue ID credentials to displaced groups).
- Occasionally, asylum seeker and refugee IDs are processed through a government body whose issued credentials are not recognized by the telecommunications or financial regulator and as such are not valid for accessing a SIM card or opening a bank account. In other cases, UNHCR-issued ID credentials are not deemed to be legally valid for accessing mobile and financial services. Inclusion of displaced persons' ID credentials in all relevant frameworks would help to avoid these issues.
- Displaced persons' ID credentials may be suitable to register a SIM card but unsuitable for accessing a bank account or mobile money service, thus stunting financial inclusion efforts. Harmonization is key. Access may be further catalyzed by tiering ID requirements according to a risk-based approach, for example by providing a basic level of service to those whose identities have been minimally authenticated and a broader range of services following more extensive ID verification.
- When legal access is not an option, for example in emergency situations, workarounds are sometimes an operational necessity, though they bring risk to both humanitarian organizations and end users.

UNHCR is keen to build on this research by establishing country-level advocacy platforms in partnership with the GSMA and others to develop constructive agendas for the inclusion of displaced groups with governments, humanitarian and development agencies, mobile operators, and financial service providers alike.

Acknowledgments

The author, Dr. Aaron Martin, would like to thank the following individuals for the thoughtful conversations during the course of the research, as well as for feedback provided on various iterations of the ideas within the report: Kevin Donovan, Rodrigo Firmino, Philippe Frowd, Juma Kasaha, Tim Kelly, Bronwen Manby, Fredesvinda Fatima Montes, Hellen Mukiri-Smith, and Linnet Taylor.

He also thanks Talita Cetinoglu and Volkan Yilmaz for organizing a panel on ***Rethinking Cash Assistance within Humanitarian Response*** at the 2018 World Conference on Humanitarian Studies, where aspects of this research were presented, and Mohamed Farahat and Ian Brown for the invitation to present parts of the work at a roundtable on ***Refugees Digital Rights: Necessities and Needs*** at the 2018 Internet Governance Forum. We would also like to thank the participants who attended the side meeting on ***Enabling Access to Mobile Connectivity*** at the World Economic Forum 2019 Annual Meeting in Davos, where these ideas were discussed.

This author is indebted to innumerable UNHCR staff, interviewees, and survey respondents without whom this research would have been impossible. In particular, he would like to acknowledge John Warnes, Nicholas Oakeshott, Hanna Mattinen, Micol Pistelli, Sana Khan, Sara Tholozan, Nur Amalina Abdul Majit, Chris Earney, Hans Park, Giulia Balestra, Agnes Schneidt, Katie Drew, and Rebeca Moreno Jimenez for their support during the research and drafting. He would also like to thank Kyla Reid, Yiannis Theodorou, and Erdoo Yongo from the GSMA for their stimulating conversations, willingness to share data in the early stages of the research, and feedback on the first drafts of the report.

Abbreviations

AML	Anti-Money Laundering
APG	Asia/Pacific Group on Money Laundering
ARRA	Administration for Refugee-Returnee Affairs
ATM	Automatic Teller Machine
BEAC	Banque des États de l'Afrique Centrale
BCEAO	Banque Centrale des États de l'Afrique de l'Ouest
BTRC	Bangladesh Telecommunication Regulatory Commission
CANIF	Commission d'Analyse des Informations Financières
CAR	Central African Republic
CDD	Customer Due Diligence
CENAREF	Cellule Nationale des Renseignements Financiers
CFT	Combating the Financing of Terrorism
CGM	Commisariat General des Migrations
CIR	Carte d'Identité du Réfugié
CNARR	Commission Nationale d'Accueil de Réinsertion des Réfugiés et des Rapatriés
CNR	Commission Nationale pour les Réfugiés
CPF	Cadastro de Pessoa Física
CTD	Convention Travel Document
DGMM	Directorate General of Migration Management
DNFBP	Designated Non-Financial Businesses and Profession
DOR	Department of Refugees
DRC	Democratic Republic of Congo
EACO	East African Communications Organization
ECOWAS	Economic Community of West African States
EIRS	Equipment Identity Registration System
EDD	Extended Due Diligence
eKYC	electronic Know Your Customer
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
ETM	Emergency Transit Mechanism
FATF	Financial Action Task Force
FCU	Financial Crime Unit
FIU	Financial Intelligence Unit
FSP	Financial Service Provider
G7	Group of 7
GABAC	Groupe d'Action contre le blanchiment d'Argent en Afrique Centrale
GIABA	Inter-Governmental Action Group against Money Laundering in West Africa
GSMA	GSM Association
ICRC	International Committee of the Red Cross
ICT	Information and Communications Technology
ID	Identification

IDP	Internally Displaced Person
IMEI	International Mobile Equipment Identity
IOM	International Organization for Migration
ITU	International Telecommunications Union
KRA	Kenya Revenue Authority
KYC	Know Your Customer
MENA	Middle East and North Africa
MENAFATF	Middle East and North Africa Financial Action Task Force
MFI	Microfinance Institute
MNO	Mobile Network Operator
MOI	Ministry of Interior
MRC	Mandate Refugee Certificate
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
NCC	National Communications Commission
NGO	Non Governmental Organization
NIDA	National Identification Agency
NIRA	National Identification and Registration Authority
NIN	National Identity Number
ONPRA	Office National de Protection des Réfugiés et Apatrides
OPM	Office of the Prime Minister
proGres	Profile Global Registration System
PRIMES	Population Registration and Identity Management Ecosystem
QR	Quick Response
RIMS	Refugee Information Management System
RSD	Refugee Status Determination
RURA	Rwanda Utilities and Regulatory Authority
SIM	Subscriber Identity Module
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UCC	Uganda Communications Commission
UNCDF	United Nations Capital Development Fund
UNHCR	UN Refugee Agency
VRF	Voluntary Repatriation Form
WFP	World Food Programme
ZICTA	Zambia Information and Communications Technology Authority

1. Introduction

In its 2016 *Connecting Refugees* report, UNHCR identified a number of barriers to connectivity for refugees in urban, camp, and rural settings, including among others, a lack of affordable devices and mobile services, poor literacy, weak network signal strength, misunderstandings among refugees about service plans, lack of accessible language content, challenges with charging devices, perceived lack of interest in/need for connectivity, restrictions imposed by family members on device use, privacy and security concerns, and regulatory restrictions.[1] The final of these—regulatory restrictions—can erect policy barriers to the availability of connectivity by making it more difficult for displaced persons to access services. Included among the report's planned strategic interventions was a point to "advocate to governments… to reduce regulatory barriers preventing refugees from accessing connectivity (e.g. looser identification requirements to obtain SIM cards). Working to reduce regulatory barriers is applicable to both rural and urban refugees."

These were timely insights, but since 2016 the scope of the impacts of these regulatory barriers on refugees and other displaced populations has become even more apparent. UNHCR and its partners continue to encounter ID-related policy challenges as part of humanitarian programming across numerous countries. As applications and services have advanced, enduring obstacles become impediments to an even broader array of uses. For instance, while inappropriately rigid ID requirements can create barriers to mobile connectivity, they can also impede access to financial services, including transformative innovations such as mobile money.[2]

The laws and regulations driving these demands for prescribed ID credentials differ in their policy origins and motivations: SIM registration is a telecommunications regulatory trend that has been widely embraced by governments in the Global South, where pre-paid access is predominant; in contrast, Know Your Customer (KYC)/Customer Due Diligence (CDD) requirements arise from recommendations by a relatively unknown intergovernmental organization known as the Financial Action Task Force and are realized by Central Banks and other financial regulators at national level. Nevertheless, the impacts of their implementation can be quite devastating to the undocumented and for people whose ID credentials are not recognized for these purposes. A refugee who cannot legally activate a mobile connection, open a bank account or access a mobile money wallet in his or her own name may become further marginalized and disempowered as access to information, communication, and financial services, including cash assistance and transfers, is severely limited. What is at stake in enabling access for displaced persons includes self-reliance, resilience, financial independence, social inclusion, and protection.

An evidence base is strongly needed to inform appropriate action. This report therefore focuses on a relatively under-explored, but nonetheless significant barrier to access among refugees and other displaced persons: legal and regulatory requirements mandating that an individual's ID is authenticated before accessing a mobile connection, bank account or mobile money wallet. This research is the first of its kind to systematically understand and address the combination of these challenges.

Populations of Concern

As this study addresses these legal aspects of ID and registration, it is important to carefully distinguish the various populations for whom different forms of ID may or may not be available in a given country context. UNHCR defines its persons of concern as follows[3]:

- **Asylum seekers** are individuals who have sought international protection and whose claims for refugee status have not yet been determined, irrespective of when they may have been lodged.
- **Refugees** include individuals recognized under the 1951 Convention relating to the Status of Refugees; its 1967 Protocol; the 1969 Organization of African Unity Convention Governing the Specific Aspects of Refugee Problems in Africa; those recognized in accordance with the UNHCR Statute; individuals granted complementary forms of protection; or those enjoying temporary protection. Since 2007, the refugee population also includes people in a refugee-like situation, most of whom were previously treated as others of concern.
- **Internally displaced persons (IDPs)** are people or groups of individuals who have been forced to leave their homes or places of habitual residence, in particular as a result of, or in order to avoid the effects of armed conflict, situations of generalized violence, violations of human rights, or natural or man-made disasters, and who have not crossed an international border.
- **Returned refugees (or returnees)** are former refugees who've returned to their country of origin spontaneously or in an organized fashion but are yet to be fully integrated. Return would normally only occur in conditions of safety and dignity.
- **Returned IDPs** refer to those IDPs who were beneficiaries of UNHCR's protection and assistance activities and who returned to their areas of origin or habitual residence.
- **Stateless persons** are defined under international law as persons who are not considered as nationals by any state under the operation of its law. In other words, they do not possess the nationality of any state.
- **Others of concern** refers to individuals who do not necessarily fall directly into any of the groups above, but to whom UNHCR extends its protection and/or assistance services, based on humanitarian or other special grounds.

1 UNHCR, *Connecting Refugees*, p. 14

2 This report understands mobile money based on the GSMA Code of Conduct for Mobile Money Providers (version 3) 2017 definition (p.11): A service is considered a mobile money service if it meets the following criteria: a) it includes transferring money and making payments using the mobile phone, b) must be available to the unbanked (e.g. people who do not have access to a formal account at a financial institution), c) must offer at least one of the following products: domestic or international transfer, mobile payment, including bill payment, bulk disbursement, and merchant payment, or storage of value, d) must offer an interface for initiating transactions for agents and/or customers that is available on mobile devices, and e) must offer a network of physical transactional points outside bank branches and ATMs that make the service widely accessible to everyone. Mobile banking services that offer the mobile phone as just another channel to access a traditional banking product are not included. Payment services linked to a traditional banking product or credit card, such as Apple Pay and Google Wallet, are not included.

3 Persons of concern to UNHCR: http://www.unhcr.org/ph/persons-concern-unhcr

To provide a sense of the size of these populations and the potential scale of the legal access problem, as of the end of 2017, UNHCR had counted 71.44 million persons of concern globally, including over 19.94 million refugees, 3.09 million asylum seekers, 39.11 million IDPs, 4.89 million returnees, 2.79 stateless persons, and 1.59 million others of concern. Global figures have increased every year since 2010.[4]

This research focuses on the situation of asylum seekers, refugees, and returnees.[5] Although the protection of stateless persons who have not been forcibly displaced is an integral part of UNHCR's core mandate, they have not been included in the scope of the research as a result of the limitations on existing data and project resources. Likewise, IDPs and others of concern are not explicitly included in the analysis, although it has been observed that in several countries IDPs can face greater barriers to access than refugees due to the lack of availability of appropriate ID credentials. Similarly, the research was unable to consider the situation of host communities, whose importance in addressing the challenges of displacement is being increasingly recognized.[6]

Finally, due to limitations in scope and resources, the research has not unpacked demographic considerations such as gender and age. While telecommunications and financial regulations generally do not take into account such issues, specific barriers may exist for different demographic groups in certain contexts, which would need to be further examined.

Research Questions

The main research questions driving the research[7] are:

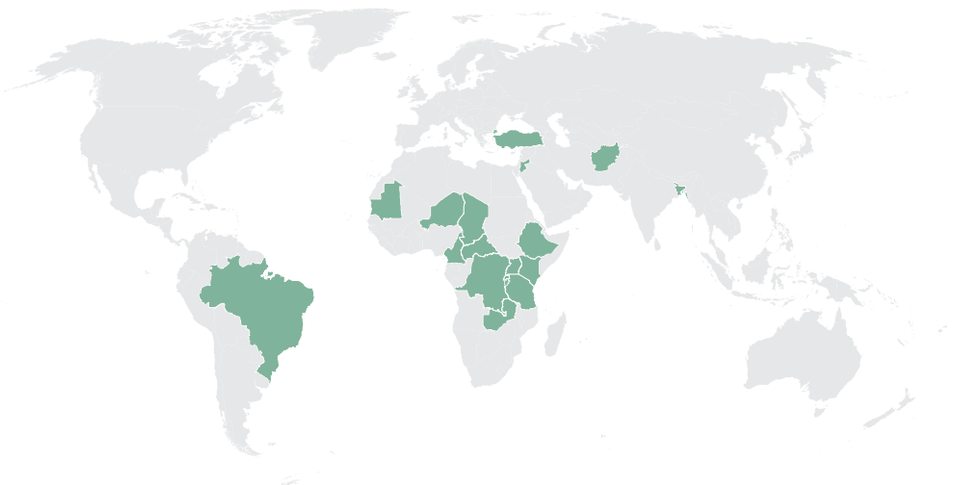
1. What legal and regulatory barriers related to ID exist for asylum seekers, refugees, and returnees to access mobile connectivity, bank accounts, and mobile money across 20 selected countries?[8]
2. What policy, regulatory, and operational good practices can be identified to mitigate these access barriers?
3. What strategic engagement and advocacy opportunities exist at national, regional, and global levels to improve the regulatory environment and State practice to facilitate inclusion?

Structure of Report

This report proceeds as follows: The next chapter discusses the benefits of connectivity, financial inclusion, and government-recognized ID credentials for populations of concern and for areas where they live. The report then reviews the two regulatory drivers that motivate the need for additional evidence and analysis: SIM registration and Know Your Customer (KYC)/Customer Due Diligence (CDD) requirements. The analysis provides a summary view into good practices and examples of challenges faced by displaced populations with respect to SIM registration and KYC/CDD policies and practices. Among the report's key findings are both operational and policy insights. The report makes recommendations to both governments and humanitarian and development organizations, including UNHCR, before concluding with reflections on emerging issues and future research to reduce barriers to accessing connectivity and financial services. This report is accompanied by a series of country reports which detail the state of laws and regulations requiring proof of ID across the 20 countries that were part of the study.

Intended Audience

This report is targeted at a wide audience: State bodies such as national telecommunications and financial regulators (including Central Banks and financial intelligence units), national refugee agencies, and national ID authorities, as well as legislatures; intergovernmental bodies such as the Financial Action Task Force (FATF) and regional associates; telecommunications policy bodies like the East African Communications Organisation; development partners such as the World Bank and funders; humanitarian agencies such as UNHCR, World Food Program, and the International Committee of the Red Cross, as well as non-governmental organizations; financial service providers, mobile network operators, and relevant trade bodies such as the GSMA; and other organizations that work to provide displaced persons with access to connectivity or financial services. We appreciate that this research represents an initial foray into the subject matter and that it will undoubtedly raise more questions for each stakeholder that warrant further study.



4 UNHCR Population Statistics: http://popstats.unhcr.org/en/overview

5 The term 'displaced' is used in the report as a catch-all to capture these groups. Where necessary, more nuanced terms are used

6 See, for example, World Bank, *Forcibly Displaced.z*

7 A brief note on methods: The research involved extensive desk research and literature reviews, interviews with experts in the humanitarian, development, and ID/registration policy domains, surveys of UNHCR country operations, and ongoing engagement with trade bodies such as GSMA as well as regulators, including at the International Telecommunications Union Global Symposium for Regulators.

8 Afghanistan, Bangladesh, Brazil, Burundi, Cameroon, Central African Republic, Chad, Democratic Republic of Congo, Ethiopia, Jordan, Kenya, Lebanon, Mauritania, Niger, Nigeria, Rwanda, Tanzania, Turkey, Uganda, and Zambia.

2. Humanitarian Context: Why Connectivity, Financial Services, and ID Matter

All too often discussions on connectivity, financial inclusion, and ID take place in isolation. This is partly to do with organizational structures within States and established ways of working within humanitarian agencies and between development partners. However, advances in technology and innovations in humanitarian assistance force us to think more holistically and comprehensively about the interdependencies across connectivity, financial inclusion, and ID, the humanitarian/development nexus, as well as the common challenges.[9] This chapter therefore develops an understanding of connectivity, financial inclusion, and ID attentive not only to key issues within each domain, but also the critical linkages.

Value of Connectivity for Displaced Persons

In 2016, the United Nations High Commissioner for Refugees conveyed in his preface to the *Connecting Refugees* report that: "A connected refugee population can play a critical role in enabling organizations such as UNHCR to innovative effectively and to improve the quality of services that we provide. Connectivity has the potential to transform how we communicate, the way in which we respond to the protection needs of displaced people, and our delivery of humanitarian services. Most significantly, better connectivity can promote self-reliance by broadening the opportunities for refugees to improve their own lives. Access to the internet and mobile telephone services has the potential to create a powerful multiplier effect, boosting the well-being of refugees and of the communities that host them."[10]

Connectivity, and in particular mobile connectivity, has the potential to mitigate the effects of forced displacement in several ways.[11] Among the benefits of connectivity to refugees and other displaced populations are:

- **Communication**: Communicating with friends and family (both in one's home and host country) has been identified as the most important need to be connected.[12] Refugees and other displaced populations arguably have a greater need for communication than the general population because displacement often separates them from their loved ones and can cause social isolation. Communication can also help with family reunification.
- **Access to information**: The benefits of access to information for refugees and other displaced populations are multifold and in some cases can be life-saving. For some, connectivity can help mitigate 'information precarity' — a condition of information instability and insecurity that may result in heightened exposure to violence — by providing people with increased access to news and other information that is most relevant to their circumstances.[13] Connectivity can also facilitate better access to information about the situation in one's home country, allowing refugees to make better informed decisions about whether and when it might be safe to return home.[14]
- **Education**: Relatedly, connectivity has been shown to yield both formal and informal education opportunities.[15]
- **Protection**: Connected refugees and others who are displaced can access security-relevant information and security-enhancing services (e.g. protection incident reporting/tracking and hotline services) provided by agencies like UNHCR. Connectivity can help streamline the asylum process by facilitating more timely communication. It can also help in terms of enhancing community-based protection by assisting populations of concern to self-organize and engage more substantially with humanitarian programming.[16]
- **Livelihood opportunities:** Being connected can increase economic opportunity in different ways. Mobile connectivity can help refugees and others create and sustain their own businesses.[17] Mobile phones help them search for market information, communicate with suppliers, and identify and connect with new customers.[18] In some cases, mobile connectivity may also allow for the possibility of working remotely, which may be important in situations where populations face constraints on the right to work or limited opportunities in the local economy.[19]
- **Social capital**: Mobile access can help bond and bridge social capital by facilitating the revival of disrupted social networks, by helping refugees search for work and maintain contact with employers, and by enabling refugees to maintain and leverage extralocal networks.[20]
- **Mental health**: There is emerging evidence of a possible relationship between refugee phone usage and mental health: A 2018 study found that each additional day a respondent used a phone the week prior to being surveyed was associated with a reduction in their probability of being depressed.[21]
- **Access to finance**: As will be discussed in the next section, access to financial services via a mobile device has proven to be one of the most important benefits of connectivity, facilitating easier access to cash, including remittances, more efficient payment methods, and other applications.

Moreover, as suggested by the UN High Commissioner for Refugees, there are connectivity benefits not just to displaced persons, but also to other humanitarian stakeholders including aid agencies, host governments, and host communities. As examples, connectivity creates two-way communication opportunities between agencies and refugees to better understand the security and health risks among the population.

9 See, for example, A. Gelb and A. Metz, *Identification Revolution: Can Digital ID Be Harnessed for Development?* and N. Oakeshott et al., *Empowering Refugees and Internally Displaced Persons through Digital Identity*: http://blogs.worldbank.org/voices/node/5636

10 UNHCR, *Connecting Refugees*, p. 5

11 There are, of course, attendant risks as well, which must be better understood and mitigated as connectivity efforts expand and deepen. For recent work in this area, see: ***The Humanitarian Metadata Problem*** report by Privacy International and ICRC (on which UNHCR was involved)

12 UNHCR, *Connecting Refugees*, p. 16

13 Campbell et al., *Syrian Refugees and Information Precarity*, p. 3

14 UNHCR, ***Connecting Refugees***, p. 28

15 GSMA, *Mobile is a Lifeline*, pp. 28-30

16 UNHCR, ***Connecting Refugees***, p. 32

17 GSMA, *Mobile is a Lifeline*, p. 23

18 Betts et al., *Refugee Economies*, p. 33

19 UNHCR, *Connecting Refugees*, p. 32

20 Göransson, *Apping and Resilience*, p. 2

21 Latonero et al., *Refugee Connectivity*, p. 27

It can also help to reduce legal non-compliance among populations by providing them with improved access to host government information.[22] Host communities may benefit economically from a connected and financially included refugee population with the capacity to transact, as well as from improved service provision in the area.

Financial Inclusion and Displacement

Financial inclusion — that is, being able to access useful and affordable financial products and services that meet one's needs[23] — is a key component of achieving protection and long-term solutions for refugees and other displaced persons.[24] Importantly, mobile is an increasingly essential modality for the delivery of financial services and promotion of financial inclusion, with mobile money in particular being especially prominent. Digital access is vital for opening up new avenues for financial inclusion. Among the benefits of financial inclusion for displaced persons are:

- **Improved livelihoods**: The *UNHCR Global Strategy For Livelihoods* explicitly includes increased access to financial services among its strategic objectives.[25] Access to financial services such as savings, credit, money transfers, and micro-insurance can improve the livelihoods of refugee populations by helping to safeguard assets, build financial capital, and plan and expand economic activities.
- **Diversified income**: Access to formal financial products and services can help refugees reduce exposure to income fluctuations by diversifying their income sources to meet basic needs, thus aiding consumption smoothing.
- **Reduced vulnerability**: Access to formal financial products can also reduce vulnerability to risky lending practices or insecure financial schemes. While not a financial product *per se* but a means to financially assist the most vulnerable, **cash-based interventions** can be leveraged to promote people's access to financial services and provide vulnerable people a way to fulfill their basic needs without resorting to harmful coping strategies.
- **Increased dignity, self-reliance, and resilience**: Financial inclusion empowers refugees and other displaced persons to meet their needs in a safe, sustainable, and dignified manner, contribute to their host economies, and prepare for their future whether they return home, integrate in their country of asylum, or resettle in a third country.[26] Economic inclusion also contributes to the self-reliance and resilience of refugees and other displaced persons, helping them to cope with economic shocks.

These benefits are, of course, contingent on the displaced being able to access to financial services. Often, however, these populations are excluded from the formal financial sector. This exclusion is primarily caused by two factors: 1) a disabling regulatory environment,

22 UNHCR, *Connecting Refugees*, p. 28
23 The World Bank, *Financial Inclusion*: http://www.worldbank.org/en/topic/financialinclusion/overview
24 AFI, *Advancing the Financial Inclusion of Refugees through an Inclusive Market System Approach*: https://www.afi-global.org/blog/2018/06/advancing-financial-inclusion-refugees-through-inclusive-market-system-approach
25 UNHCR, *Global Strategy for Livelihoods*, p. 31
26 AFI, *Advancing the Financial Inclusion of Refugees through an Inclusive Market System Approach*: https://www.afi-global.org/blog/2018/06/advancing-financial-inclusion-refugees-through-inclusive-market-system-approach

which does not sufficiently accommodate displaced populations' circumstances, e.g. their lack of recognized ID credentials or their inability to provide other documentary evidence such as proof of address or proof of work, and 2) lack of familiarity by financial service providers (FSPs) with this market segment, their livelihood opportunities, their credit risk, and the business case for serving them.[27]

Moreover, when a beneficiary is unable to access formal financial services, humanitarian interventions such as cash-based interventions are less efficient, more costly, and less secure for the beneficiary and for the aid organization, which may have to resort to setting up costly parallel structures or less secure and less accountable delivery mechanisms. Increasing access to bank accounts and mobile money services is therefore an essential element for both enhancing resilience and self-reliance of the displaced, as well as for a more effective delivery of cash-assistance.

ID as an Enabling 'Golden Thread'

Globally, more than 1 billion people lack government-issued credentials to prove their identity,[28] which can result in their continued social, economic, and political exclusion. States have committed to address this gap with *Sustainable Development Goals, Target 16.9* aiming to provide legal identity for all by 2030, including birth registration.

For vulnerable and already marginalized people, the lack of an ID credential constitutes a constant risk. For asylum seekers, refugees, and returnees, the risks are even greater. Lack of ID credentials can be both the consequence and a cause of forced displacement. ID credentials originally issued by refugees' countries of origin can be lost or destroyed during flight or as a result of the conflict which led to displacement. At the same time, refugees who are not issued with ID credentials by their host country often cannot prove their right to remain and risk being deported to face persecution. [29]

The main risks for refugees and other displaced populations without government-recognized ID credentials include[30]:

During displacement:

- Inability to move within a country or to cross international borders legally
- Vulnerability to extortion and trafficking
- Deaths unrecorded and unnotified to families
- Difficulties in establishing refugee status and increased risk of deportation
- Inability to clarify / prove familial relationships

27 Pistelli, *Removing Barriers to Access to Finance for Refugees*: http://www.findevgateway.org/blog/2017/mar/removing-barriers-expand-access-finance-refugees
28 The World Bank, *The Global Identification Challenge*: https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity
29 Manby, *Identification in the Context of Forced Displacement*, p. 1
30 Manby, *Identification in the Context of Forced Displacement*, p. 9

In the host country:

- Limited protection of individual rights, such as freedom of movement, and the risk of abuse or exploitation such as arbitrary arrest and detention
- Limited access to services and benefits, including mobile connectivity, finance, and social protection schemes
- Inability to document life events (births, marriages, etc.)
- Inability to prove legal residence on the territory, creating the risk of *refoulement* and preventing solutions

Returning home:

- Inability to repatriate, because of difficulty proving nationality, especially for children of refugees born in the host country
- Difficulty in maintaining a recognizsed family unit
- Difficulty obtaining ID credentials in the home country
- Difficulty claiming access to services, including social protection
- Difficulty reclaiming property and other rights
- Post-conflict population registries may intentionally or unintentionally exclude groups

The international protection regime requires that refugees who lack valid travel documents are issued with credentials to prove their identity by the authorities of the host State if they do not have a valid travel document. The authorities should also provide replacement documents and certificates that would usually be provided by the refugees' country of origin, but can also be provided by an internationally recognized and mandated authority, such as UNHCR.[31] While outside the scope of the study, it is worth nothing that the United Nations Guiding Principles on IDPs similarly recognize that IDPs and returning IDPs should be provided with all documents necessary for the enjoyment of their legal rights, including replacement documentation, without discrimination between men and women.[32]

States are therefore primarily responsible for registering and providing ID credentials to asylum seekers and refugees as a crucial first step in ensuring their protection.[33] In line with its mandate, UNHCR has often provided support to States, particularly in situations of mass influx by undertaking refugee registration. The organization's protection mandate provides a basis for it to undertake refugee registration and documentation where States are unable or unwilling to do so. In addition, UNHCR also supports States through the joint use of the digital tools contained in UNHCR's Population Registration and Identity Management Ecosystem ("PRIMES"), including its biometrics systems.[34]

Many States, particularly in Africa, are increasingly taking more responsibility for refugee registration and are considering including refugees in foundational ID platforms, where

31 See, for example, 1951 Convention on the Status of Refugees, Articles 25 & 27
32 UN Guiding Principles on Internal Displacement 1998, Principle 20
33 UNHCR Executive Committee Conclusion on Registration of Refugees and Asylum Seekers, No. 91 (LII) - 2001
34 See UNHCR PRIMES: https://www.unhcr.org/primes.html

they exist or are under development. In some states, particularly those with Integrated Population Registration Systems, consideration is being given to interoperability between functional refugee registries and national registries, for example, to facilitate the de-duplication of refugees from citizens and vice-versa in relevant registries. In light of States taking increasing responsibility for refugee registration, there are growing opportunities for greater government recognition of the ID credentials issued to registered refugees and to promote their greater inclusion in mainstream ID systems.

These approaches, recognized in the Global Compact on Refugees[35] (adopted in late 2018), can result in States being provided with a clearer picture of who lives on their territory, create efficiencies in distributing assistance, and prevent fraud. On the other hand, refugees and other displaced persons can expect to receive recognized ID credentials which can increase their access to services and protection. They are also consistent with the establishment of Integrated Population Registration Systems.

ID is no longer just paper-based and centered on breeder documents, such as birth certificates and ID cards. The concept is broadening to include digital ID, enabled by new technologies like smart cards and biometrics, allowing individuals to authenticate their ID electronically such as though electronic KYC (whereby, for example, an individual's biometrics are verified by querying a data store to authenticate his or her identity). These developments increasingly facilitate transactions in the digital sphere. UNHCR believes displaced persons should also have access to a digital ID, which can help further facilitate access to connectivity and financial services, as well as broader digital inclusion. This aligns with the G20 High Level Principles on Digital Finance, Principle 7, which calls for States to "facilitate access to digital financial services by developing, or encouraging the development of, customer identity systems, products and services that are accessible, affordable, and verifiable and accommodate multiple needs and risk levels for a risk-based approach to customer due diligence".[36]

35 Global Compact for Refugees, Final Draft, paragraphs 58 and 82: https://www.unhcr.org/events/conferences/5b3295167/official-version-final-draft-global-compact-refugees.html
36 G20 High-Level Principles for Digital Financial Inclusion: https://www.gpfi.org/publications/g20-high-level-principles-digital-financial-inclusion

3. Policy Background: ID Mandates

This report focuses on the legal and regulatory barriers to displaced persons' access to both mobile and financial services, specifically bank accounts and mobile money; in particular, it examines how legally mandated ID requirements that do not accommodate the situations of displaced persons may impede access to both connectivity and finance.

Two ID policy trends are especially notable and can restrict access: 1) Subscriber Identity Module (SIM) registration requirements, which fall within the remit of national telecommunications regulators, and 2) Know Your Customer (KYC)/Customer Due Diligence (CDD) rules propagated by Central Banks and financial regulators, aiming to implement global recommendations, for the purposes of preventing money laundering and terrorist financing, among other illicit financial activity. This chapter explains the policy motivations, core requirements, and general impacts of both SIM registration and KYC/CDD mandates.

Evolution of SIM Registration Requirements

For years, anonymous mobile connectivity was a fact of life in many parts of the world, particularly where the prepaid model of access is predominant. The purchase and use of a SIM card—and in some cases, multiple SIM cards from different network providers in order to utilize the cheapest tariffs —without legally-required proof of ID was the norm. Indeed, the ease with which a mobile connection could be activated in many parts of the world was a key contributing factor to the rapid global growth of mobile telephony.

However, over the past decade governments around the world have implemented legal requirements that mandate subscribers to provide proof of ID in order to activate and use a SIM card.[37] According to the GSMA, as of February 2018 SIM registration was mandatory in 147 countries.[38] This regulatory trend has been most acute in jurisdictions in Africa. Prior to 2006, no African country mandated SIM registration — across the continent one was able to purchase a prepaid card and use it more or less anonymously[39]; whereas as of July 2018, only a handful countries had not introduced mandatory SIM registration into law.

SIM registration regulations generally specify which forms of ID credential are acceptable to activate a SIM card, timelines for registering a SIM after its purchase, and any penalties, either for operators and their agents or for customers who flout the rules. While enforcement of SIM registration rules was notoriously lax following the initial wave of government mandates, MTN Nigeria was famously fined $5.2 billion USD in October 2015 for failing to comply with a government order to disconnect improperly registered SIM cards.[40] Operators have since started enforcing SIM registration rules much more stringently,

37 GSMA, *Mandatory Registration of Prepaid SIM Cards*, p. 2
38 GSMA, *Access to Mobile Services and Proof-of-Identity*, p. 48
39 Donovan & Martin, *The Rise of African SIM Registration*
40 BBC News, Nigeria Telecom Giant MTN Fined a Record $5.2bn: https://www.bbc.com/news/business-34638595

while governments continue to crack down on non-compliance, most recently in Kenya.[41] In many jurisdictions SIM registration practices are still manual and involve taking photocopies or digital scans (stored locally) of a customer's ID credentials, often without additional authentication, such as verifying the credential against an issuing government agency's database. The lack of digital verification processes is due to the fact that ID infrastructures in these countries are immature.[42] Commonly accepted forms of ID credential include national ID cards, passports, work permits, voter ID cards, and other government-issued documentation. However, advancements in ID technology are changing SIM registration processes, which increasingly involve the real-time verification of identity information against government databases and the collection (and sometimes authentication) of biometric information. As examples, Thailand[43] and Bangladesh[44] have introduced biometric checks for SIM cards. In Kenya, Safaricom has decided to voluntarily incorporate a biometric component to its SIM registration efforts (based on thumbprints) to prevent SIM swap fraud.[45]

While it is outside the scope of this report to interrogate the efficacy of SIM registration mandates globally, understanding their motivations may be instructive. Proponents of SIM registration often justify the measures on security grounds. Efforts are sometimes organized at the regional level: In East Africa, for example, the East African Communications Organization (EACO) continues to support regional SIM registration efforts, encouraging national governments in the region to adopt and enforce relevant laws and regulations.[46]

Other reasons for the pursuit of SIM registration are less well-publicized but nonetheless noteworthy: the International Telecommunication Union (ITU) in 2007 recommended SIM registration to improve statistical accuracy on the mobile market.[47] The emergence of different forms of fraud, including SIM boxing[48] and unauthorized SIM swaps resulting in mobile money wallets being breached, have also recently catalyzed SIM registration mandates.

To the extent that users have access to the required ID credentials, mobile network operators may benefit from government mandates for SIM registration, despite the

41 Musyoki, *Communications Authority of Kenya Notice on SIM Card Deactivation*: https://www.kenyans.co.ke/news/29826-communications-authority-kenya-ca-notice-sim-card-deactivation
42 According to GSMA, as of February 2018, 85% of countries mandating SIM registration only require MNOs to capture and store a record of the required identification credentials; 4% of countries require MNOs to capture and proactively share this information with a government agency; and 11% of countries have mandated a 'capture, validate, and store' model whereby MNOs are required to validate the document presented and/or biometric details of the customer, usually by querying a central government database, before storing this information. In some cases, MNOs are charged a fee to validate a customer's identity credential against a government database: *Access to Mobile Services and Proof-of-Identity*, p. 28
43 Reuters, *Thailand to Roll Out Biometric Checks for SIM Cards Nationwide*: https://www.reuters.com/article/us-thailand-telecoms/thailand-to-roll-out-biometric-checks-for-sim-cards-nationwide-idUSKBN1D611A
44 Ahmed et al., *Privacy, Security, and Surveillance in the Global South*, p. 909
45 Musyoki, *Safaricom to Use Thumbprint Identification to Prevent SIM Swap Fraud*: https://www.kenyans.co.ke/news/32281-safaricom-use-thumbprint-identification-prevent-sim-swap-fraud
46 Among the objectives of EACO's Working Group 1 is "to develop a regulatory framework for implementing SIM card registration within EAC Member States": http://www.eaco.int/pages/working-groups
47 TeleGeography, *ARTP Senegal Extends Deadline for SIM Registration*: https://www.telegeography.com/products/commsupdate/articles/2013/08/05/artp-senegal-extends-deadline-for-sim-registration/
48 A form of telecommunications fraud by which calls made via the Internet are redirected onto mobile networks via machines that house SIM cards (thereby avoiding payment of call termination fees)

upfront compliance costs associated with registering users. This is because registration, which can be burdensome and time-consuming, imposes switching costs and arguably reduces 'customer churn', the industry term for migration to competitors.[49] Regardless of their motivations, the impact of SIM registration policies has been well documented. In most markets, subscriber numbers have fallen after registration mandates have gone into effect, largely due to unregistered lines being disconnected.

Globalization of ID Requirements for Financial Services

The emergence and widespread global adoption of recommendations for identifying and verifying a customer's identity in order to access financial services has followed a different policy trajectory than SIM registration requirements—one with origins in the Group of 7 (G7). Established in 1989 by the G7, the Financial Action Task Force (FATF) is an inter-governmental body whose objectives include setting standards, making policy recommendations, and promoting effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, and other threats to the integrity of the international financial system.

The FATF has developed a series of Recommendations that are widely recognized as the international standard for anti-money laundering (AML) and combating the financing of terrorism (CFT). First issued in 1990, the FATF Recommendations were revised in 1996, 2001, 2003, and most recently in 2012 to ensure that they remain up to date and relevant to the realities of financial crime prevention. As its Recommendations are non-binding, the FATF strives to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.[50]

The FATF Recommendations are the leading source of risk-based standards for Know Your Customer (KYC) and Customer Due Diligence (CDD) measures in the AML/CFT context. The Recommendations for KYC/CDD state that certain measures should be undertaken when business relationships are established or relevant occasional transactions are undertaken (e.g. transactions are made over a certain amount), to include:

- Identifying the customer and verifying ID using reliable, independent source documents
- Obtaining information on the purpose and intended nature of the business relationship
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds
- Enhanced Due Diligence (EDD) is required for higher risk customers, relationships, and transactions, while reduced or simplified measures may suffice where the risks are lower[51]

49 Jentzsch, *Implications of Mandatory Registration of Mobile Phone Users in Africa*, p. 617
50 FATF, *Who We Are*: http://www.fatf-gafi.org/about/whoweare/
51 FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, p.12

These high-level Recommendations are intended to be implemented by members at the national level through legislation and other legally binding measures, which are overseen by Central Banks and national financial regulators. National implementations stipulate the specifics of ID verification to be performed as part of KYC/CDD in the jurisdiction, based on the realities of the local context, such as which forms of ID are commonly available to customers.

Cognizant of the potentially negative impacts of AML/CFT and KYC/CDD on financial inclusion, the FATF has made occasional adjustments to its framework to soften the impact on access to financial services within its risk-based approach, particularly by introducing 'progressive', 'proportional' or 'tiered' KYC/CDD requirements.[52] A tiered approach to KYC has proven popular among some governments because it allows regulators to distinguish between lower risk and higher risk scenarios, thereby permitting KYC procedures to be tailored to the specific risks posed by different types of customers and transactions.[53]

FATF classifies non-bank mobile money providers as 'money or value transfer services providers', which means mobile money providers must comply with certain KYC/CDD measures and record keeping, monitoring, and reporting requirements.[54] In countries in which mobile money has been widely adopted, governments have also started issuing guidance to clarify KYC/CDD regulatory expectations for these platforms. It has been realized that mobile money can present a regulatory challenge as it implicates both telecommunications and financial regulations, making coordination between these agencies necessary for effective oversight.

Finally, it is important to note that while humanitarian agencies are not directly subject to the KYC/CDD rules found in AML/CFT regulations (due to the fact that they are not financial institutions), they do apply to the financial service providers with which humanitarian agencies partner to deliver cash transfers[55], in addition to financial service providers with direct relationships with persons of concern.

52 Noor, *Anti-Money Laundering Regulation and Financial Inclusion*: http://www.cgap.org/blog/anti-money-laundering-regulation-and-financial-inclusion
53 GSMA, *Proportional Risk-based AML/CFT Regimes for Mobile Money*, p. 7
54 GSMA, *Proportional Risk-based AML/CFT Regimes for Mobile Money*, p. 30
55 ELAN, *Humanitarian KYC Case Studies*

4. Analysis

Previous chapters detailed the humanitarian context with a focus on the benefits of connectivity, financial inclusion, and digital ID initiatives, and summarized the ID policy trends embodied in SIM registration mandates and Know Your Customer/Customer Due Diligence requirements for financial services. This chapter comparatively analyzes the state of legal and regulatory ID-related barriers affecting populations of concern across 20 countries.

Table 1: Countries Studied by Region

Europe	MENA	Asia and the Pacific	East Africa and Great Lakes	Southern Africa	West and Central Africa	Americas
Turkey	Lebanon	Afghanistan	Burundi	DRC	Niger	Brazil
	Jordan	Bangladesh	Ethiopia	Zambia	Nigeria	
	Mauritania		Kenya		Cameroon	
			Rwanda		CAR	
			Tanzania		Chad	
			Uganda			

Before proceeding, there are three important caveats to acknowledge: First, significant discrepancies often exist between what the law says with respect to ID requirements and what occurs in practice. Second, these issues are incredibly nuanced and complex, with different populations of concern facing different challenges across and within jurisdictions; while this chapter presents a summary view of these challenges, the individual country reports capture much of the specific details. Third, the policy environment in these countries is highly dynamic, therefore it is possible that the specifics of laws and regulations, or their implementation, have changed since the research was conducted from August to December 2018.

Access to ID Credentials

Understanding the extent to which asylum seekers, refugees, and returnees can legally access connectivity, bank accounts, and mobile money requires us first to understand their ability to access recognized ID credentials in host states (and, in the case of returnees, their country of origin as well). This will depend on a number of factors, including a) the registration and documentation processes for these groups in the host state, particularly the body responsible (e.g. UNHCR or the government), b) which forms of ID credential the population of concern or individuals possess, including credentials brought with them from the country of origin (e.g. some refugee populations are exceptionally able to travel with passports) and, c) the extent to which the credentials held are recognized by the government as a matter of national law and regulation.

UNHCR categorizes the responsibility for asylum seeker and refugee registration into the following types (although there are sometimes crossovers between these categories):

- **UNHCR-only registration** usually takes place in States which are not signatories to the 1951 Refugee Convention, where there is no appropriate national legal framework for refugee protection, and/or where the State may have limited will or capacity to perform registration functions. In these cases, States may allow UNHCR to conduct registration for the whole population of concern and issue documentation under its mandate. Examples include Malaysia and Thailand.
- **Joint registration** is an arrangement whereby UNHCR works in partnership with governments to expand the protection space for persons of concern by supporting and strengthening national registration and documentation systems and capacities of States. This partnership can take many forms and may be led by UNHCR or the government depending on legal, institutional, procedural, and operational capacities. UNHCR may provide material, financial, technical, and/or human resource support for registration activities, as well as legal support in relation to accession to international legal instruments, development of domestic legislation, and/or national structures. Joint registration is collaborative, based on common purpose in the collection, processing, and transfer of data, with shared procedures such that UNHCR and government actors might collect and process different data in relation to the same individual record at different stages of a case management process. In joint registration activities with government authorities, a formal agreement outlines procedural standards and safeguards for registration, roles, and responsibilities, as well as provisions relating to data protection. Examples include Rwanda and Ethiopia.
- **Parallel registration** arises where UNHCR and government authorities have distinct procedures for registering asylum seekers, often for different purposes, and therefore collect and manage different datasets. Parallel registration sometimes takes place at the outset of an emergency or while government and UNHCR negotiate more efficient arrangements. Parallel registration may also occur following a transition of registration activities to the host State while UNHCR continues to register a subsection of the population to facilitate activities under UNHCR's mandate, for instance, registration for the purposes of protection and assistance and/or solutions, such as resettlement. Examples include Jordan and Ukraine.
- **Split registration** is usually an exceptional arrangement in which UNHCR registers persons of a certain profile and the government registers others, based on agreement with the government and relevant national laws. Processes and data sets may or may not be the same. This could also be a temporary arrangement in a transition process where the government decides to discharge its registration responsibility in relation to a subset of the population initially with a view to eventually assuming the responsibility for the whole population over time. This approach used to be the case in Turkey, however the government has recently taken over responsibility for the registration of Syrians and non-Syrian refugee populations.

- **Government-only registration** indicates that transition from UNHCR to government registration has either taken place in the country or UNHCR is not otherwise responsible for registration. UNHCR's involvement in registration activities may be limited to its supervisory role under Article 35 of the 1951 Convention. In exceptional circumstances, such as an emergency, UNHCR may be asked to provide operational support to the government, such as a one-off registration exercise. Examples include Brazil and North Macedonia.

However, it is important to note that refugees may be entitled to be enrolled in State foundational ID platforms being established in a number of countries including Côte d'Ivoire, Guinea, and Morocco. In some cases, enrollment may not be dependent on registration as a refugee or determination of refugee status.

In general, though by no means universally, the registration and documentation process for asylum seekers, refugees, and returnees[56] is as follows:

- **Asylum seekers** may arrive to a host country with no or minimal ID credentials (some individuals and occasionally particular profiles possess ID credentials from the country of origin, including a passport, ID card, birth certificate, driver's license or voter card). However, these ID credentials cannot be verified with the country of origin. In some countries, particularly where UNHCR maintains a role, a pre-registration token may be issued to asylum seekers prior to registration. Upon registration, asylum seekers will be issued with an asylum seeker certificate or equivalent document. Individual photographs are taken and refugees can be enrolled in biometric systems to facilitate identification and authentication as part of case processing and, where appropriate, the distribution of assistance.
- **Refugees** can be recognized after a variety of processes which are adopted depending on their situation (such as *prima facie* determination, accelerated Refugee Status Determination (RSD), simplified RSD or regular RSD). Those who are processed through regular RSD will usually be issued with a refugee ID card or certificate, but the issuing authority will depend on the configuration at the national level. UNHCR promotes that ID credentials issued to refugees and the determination of their status should be provided by host governments, consistent with the national legal framework. This can be the case even where UNHCR has undertaken the determination of refugee status under its mandate. Under the 1951 Convention, States are required to issue travel documents to refugees who do not have valid passports and who are lawfully staying, subject to a number of qualifications.[57] Like asylum seekers, refugees are increasingly enrolled in biometric systems to facilitate identification and authentication as part of case processing and, where appropriate, the distribution of assistance.

56 More details are available in UNHCR's Guidance on Registration and Identity Management: https://www.unhcr.org/registration-guidance; due to scope limitations, IDPs, returned IDPs, stateless persons, and others of concern are not explicitly included in the analysis. However, it has been observed that in several countries IDPs can face greater barriers to access than refugees due to the lack of availability of appropriate documentation. Stateless persons are also regularly marginalized due to their lack of identity documents.

57 1951 Convention, Article 28

- **Returnees** who have returned to their home country in an organized fashion usually arrive with a Voluntary Repatriation Form, which may be recognized as a travel or ID credential depending on the terms of the agreement made between the host State, country of origin, and UNHCR to facilitate return. The returnee may hold ID credentials from the country of origin issued prior to departure. Those who have returned to their country of origin spontaneously may too hold an original ID card from their home country, though they may arrive with little or no valid ID. Returnees often need to apply for a proof of ID from the home government upon their return, a process which UNHCR advocates for and supports.

Table 2: Summary of Legal Access[58]

	Mobile Connectivity			Bank Account			Mobile Money		
	Asylum Seeker	Refugee	Returnee	Asylum Seeker	Refugee	Returnee	Asylum Seeker	Refugee	Returnee
Afghanistan	N	N	Y^	N	N	S^	S	S	S^
Bangladesh	N	N	Y^	N	N	Y^	N	N	Y^
Brazil	S	Y	N/A	S	Y	N/A	N/A	N/A	N/A
Burundi	N	Y	Y^	N	Y	Y^	N	Y	Y^
Cameroon	N	Y	N/A	N	S	N/A	N	S	N/A
CAR	N	Y	Y^	N	Y	Y^	N	Y	Y^
Chad	N	Y	Y^	N	S*	Y^	N	Y	Y^
DR Congo	S	S*	Y^	N	S*	Y^	N	S*	Y^
Ethiopia	N	S*	N/A	N	S*	N/A	N	S*	N/A
Jordan	N	Y	N/A	N	S	N/A	N	Y	N/A
Kenya	N	S*	N/A	N	S*	N/A	N	S*	N/A
Lebanon	N	Y	N/A	N	N	N/A	N	N	N/A
Mauritania	N	S*	N/A	N	S*	N/A	N	S*	N/A
Niger	S	Y	Y^	S	Y	Y^	S	Y	Y^
Nigeria	N	S*	Y^	N	S*	Y^	N	S*	Y^
Rwanda	N	Y	S^	N	S	S^	N	N	S^
Tanzania	N	N	N/A	N	N	N/A	N	N	N/A
Turkey	S	S	N/A	S	S	N/A	N/A	N/A	N/A
Uganda	N	S*	N/A	N	S*	N/A	N	S*	N/A
Zambia	N	Y	N/A	N	S	N/A	N	Y	N/A

58 Table 2: Summary of Legal Access: Does the legal/regulatory framework in a given country permit the population of concern (asylum seekers, refugees, and returnees) to access the service in their own name?

Y: Yes, without any restrictions (e.g. no requirements for ID documentation) or with restrictions which can be met easily by all members of the population of concern
S: Yes, though seldomly; i.e., with restrictions which are possible but not easy to meet or which can be met by some but not all members of the population of concern
N: No
N/A: Not applicable

* with host government-issued refugee ID card/number (or equivalent)
^ once the returnee has been issued with a national ID card (or equivalent)

Refugee ID cards issued by host governments have the potential to be the most empowering form of ID for refugee populations, permitting access to a range of services, however this will depend on the national context including the regulatory framework. Returnees in possession of national ID cards are likewise more likely to be identified to access government or private sector services. However, it must be noted that in many countries considerable delays have been experienced in the issuance of these documents to asylum seekers and refugees. Moreover the credentials issued to asylum seekers and refugees, both by UNHCR and by States, are not always recognized as proof of ID to access all private or public services.

Table 2 provides a summary view of the impacts of legal and regulatory frameworks on access across the 20 countries studied. The sections that follow focus on identified regulatory good practices that facilitate legal access as well as examples of how the law can constrain access to mobile connectivity, bank accounts, and mobile money.

Access to SIM Cards

To what extent do legal and regulatory environments facilitate or constrain access to mobile connectivity, i.e. SIM cards? While SIM registration is required in all 20 countries included in the study, displaced populations' access varies widely depending on the group and host country.

None of the countries reviewed permits asylum seekers consistent legal access to SIM cards due to their lack of recognized ID credentials, though informal workarounds are common.

For refugees, compared to asylum seekers, legal access to SIMs is comparatively less restrictive in many countries. Legal access may depend on how efficiently and quickly ID credentials are issued to refugees. For example, in Ethiopia a refugee ID card jointly issued by the Administration for Refugee-Returnee Affairs and UNHCR permits legal access to a SIM card; as of January 2019, only 37% of the refugee population had been issued such an ID credential by the government, though this figure is expected to increase rapidly over 2019.

In extreme cases, such as in Bangladesh, the sale of SIMs to Rohingya refugees has been banned by the government, with severe penalties for those who contravene the ban.

Case study: Bangladesh

SIM registration is required by law in Bangladesh as specified in the *Cellular Mobile Phone Operator Regulatory and Licensing Guidelines, 2011* (see section 38 on Registration of Subscribers). Overseen by the Bangladesh Telecommunication Regulatory Commission (BTRC) within the Posts and Telecommunications Division, Bangladesh's SIM registration process requires subscribers to provide a copy of their national ID card or passport, as well as fingerprint biometrics verified against a national database (as of late 2015)[59] in order to activate a mobile connection.

It is prohibited to register more than 15 SIM cards using the same ID credential. In 2017 the BTRC proposed to reduce the number of SIM cards that can be registered to any one person from 20 to 5, but mobile network operators strongly objected on the grounds that many legitimate connections would be affected. The regulator and industry subsequently negotiated a compromise of the current cap (15 SIMs per person). The BTRC regularly blocks SIM cards that have been registered against the same ID credential in excess of this cap.[60] The BTRC imposes a $50 fine for each unregistered SIM.[61] A 2016 legal challenge against biometric SIM registration, based on privacy grounds and concerns about access by foreign entities, was unsuccessful.[62] In January 2019, BTRC launched an International Mobile Equipment Identity (IMEI) database to reduce the use of illegally imported devices.[63]

Legal access to SIM cards by refugees in Bangladesh is extremely challenging, namely due to a lack of access to required forms of ID. Moreover, the BTRC has reportedly banned the sale of SIMs to Rohingya refugees and has allegedly criminalized the provision of previously registered SIMs to Rohingya.[64] Individuals have been arrested for selling both mobile devices and SIMs to Rohingya[65] and mobile network operators have been warned not to provide connections to refugees in contravention of the law.[66] It has been reported that the government is currently developing a process to sell SIM cards to the Rohingya, though details on this process are scant.

59 bdnews24, *Bangladesh Launches Registration of Mobile Phone SIMs with Biometric Details*: https://bdnews24.com/bangladesh/2015/12/16/bangladesh-launches-registration-of-mobile-phone-sims-with-biometric-details

60 Bushell-Embling, *Bangladesh to Block 3m Registered SIMs*: https://www.telecomasia.net/content/bangladesh-block-3m-registered-sims

61 The Daily Star, *SIM Re-registration a Must in Bangladesh*: https://www.thedailystar.net/frontpage/sim-re-registration-must-139189

62 Mukut, *Biometric SIM Registration Legal*: https://www.dhakatribune.com/bangladesh/2016/04/13/biometric-sim-registration-legal

63 The Daily Star, *One-third Handsets Imported Illegally*: https://www.thedailystar.net/business/telecom/bangladesh-telecom-regulator-mobile-phone-imei-database-launched-legal-import-mobile-handset-1691311

64 bdnews24, *Bangladesh Regulator Bans Selling Mobile SIMs to Rohingya Refugees*: https://bdnews24.com/bangladesh/2017/09/23/bangladesh-regulator-bans-selling-mobile-sims-to-rohingya-refugees

65 The Daily Star, *5 Rohingyas Jailed for Selling Mobile, SIMs*: https://www.thedailystar.net/rohingya-crisis/5-rohingyas-jailed-selling-mobile-sims-1487776

66 The Daily Star, *Operators Selling SIMs to Rohingyas to Face Action*: Govt: https://www.thedailystar.net/business/operators-selling-sims-rohingyas-face-action-govt-1466884

Where returnee populations are concerned, the key to unlocking access to SIMs is acquiring a government-issued ID credential, like other citizens. However, in at least one country this has proven challenging enough that a workaround has been devised by UNHCR: For returnees in Rwanda who have yet to receive their national ID card, which can take several months to be issued, UNHCR conducts a bulk activation of Airtel SIM cards registered in the organization's name. Once the returnee obtains their national ID card, they are informed that they need to physically present it at an Airtel location to update the registration data.

Access to Bank Accounts

To what extent do legal and regulatory environments facilitate or constrain access to bank accounts? While KYC/CDD requirements have been mandated across the 20 countries under examination, some implementations are more flexible and inclusive of displaced persons, while others are far more stringent and exclusive.

Financial service providers in Niger accept government-issued refugee attestations as proof of ID to open a bank account, thus permitting some form of access for asylum seekers and refugees. While Malawi is not part of this study, it is worth pointing out that the UNHCR registration card has recently been recognized as a valid document for asylum seekers (as well as refugees) to open accounts with the New Finance Bank. However, most jurisdictions do not allow asylum seeker populations to legally access financial services (unless they are still in possession of a valid passport or national ID card from their home country, which is quite uncommon among many profiles and, in any event, can present authentication challenges).

In Uganda some financial institutions (mostly banks) seek additional clarifications or 'no objections' from the Bank of Uganda before accepting forms of ID other than passports and national IDs. To address concerns about the accuracy of registration data in Uganda, a country-wide biometric verification exercise of the asylum-seeker and refugee populations was conducted between March and October 2018. The Government of Uganda is now committed to using the appropriate tools for continuous registration, which is their responsibility, and to ensuring the integrity of the registration process. The strengthened registration and case management systems will improve service and assistance delivery. UNHCR is working closely with the Office of the Prime Minister in the roll-out of these new systems and jointly addressing obstacles that emerge in their practical application at field level.[67] Discussions are also ongoing between UNHCR and the Office of the Prime Minister to ensure connectivity between the new biometric ID cards and a limited part of the underlying database in order to allow FSPs to verify information on, for example, place of residence.[68]

In some countries access to bank accounts for refugees is rather restrictive. For example, banks in Chad do not accept refugee ID cards, issued by the Government's *Commission Nationale d'Accueil de Réinsertion des Réfugiés et des Rapatriés (CNARR)* with support

67 UNHCR, *UNHCR statement on the refugee response programme in Uganda* https://www.unhcr.org/news/press/2018/11/5c016d144/unhcr-statement-refugee-response-programme-uganda.html

68 Microfinanza, *Assessing the Needs of Refugees for Financial and Non-Financial Services* - Uganda

from UNHCR, for opening a bank account. In other countries, other documentary requirements like proof of address or proof of income can also prove to be barriers.

In Rwanda, refugees are not specifically addressed in the laws and regulations governing customer ID and authentication (a common trend across the countries studied). This has led to uncertainty, as most refugees in the camps have proof of registration documents issued by the Ministry of Disaster Management and Refugee Affairs, but lack government-issued ID cards.[69]

Case study: Lebanon

Lebanon participates in the Middle East and North Africa Financial Action Task Force (MENAFATF), which is an Associate Member of the Financial Action Task Force. Lebanon's key regulations driving KYC requirements are Law 318 Fighting Money Laundering[70] and Basic Circular No. 83 Addressed to Banks and also to Financial Institutions. Article 3 of Section II of Basic Circular No. 83 addresses relations with customers and due diligence measures, including ID requirements, which specify that a passport, ID card, individual civil registration or residence permit must be provided, as well as proof of address.

Populations of concerns regularly face obstacles in opening bank accounts aside from proving their identity: requirements for proving sources of income and residency have proven to be barriers. For this reason, UNHCR has facilitated access to banking services by issuing prepaid cash cards to beneficiaries under the name and control of UNHCR. The card can be used by designated agencies to provide assistance, however there are restrictions on the range of permissible transactions, which exclude the following: receiving deposits from other individuals, receiving remittances, online purchases, transferring funds to other accounts, etc.

In Jordan, cash assistance is provided through an ATM card and/or iris scan-based withdrawal with the Cairo Amman Bank. However, cash cannot be stored on the card and money has to be withdrawn or used by the refugee within a limited time frame.

Generally speaking, for returnees, access to bank accounts and other financial services is only possible once access to a national ID card or equivalent valid proof of ID is secured.

It is important to stress that even when regulation allows refugees to open a bank account with their government-issued or UNHCR ID, local banks are sometimes not informed or

69 FSDA, *Refugees and Their Money*

70 Shahin, *Compliance with International Regulation on AML/CFT: The Case of Banks in Lebanon*

have yet to adapt internal procedures. Some banks may still require fixed addresses as part of their due diligence, which recently-arrived refugees often do not have.

When it comes to access to credit provided by microfinance institutions (MFIs), regulatory requirements can be less restrictive. Several MFIs[71] in a number of countries such as Jordan, Lebanon, Uganda, Rwanda, Morocco, Tunisia, and Argentina have started providing loans to refugees by accepting UNHCR ID or the ID issued by governments to refugees, using alternative ways to verify residence and credit scoring. What has proven to be a key enabler to facilitate access to these services was the work done by UNHCR and partners to raise awareness about the financial needs of refugees with FSPs in the country. This advocacy work is fundamental and could be replicated in other countries to ensure greater access to a broader range of financial services by refugees.

Access to Mobile Money

To what extent does the regulatory environment facilitate or constrain access to mobile money?

As with SIM registration, of the 20 countries examined, none extend consistent legal access to mobile money to asylum seekers, though workarounds are regularly reported. However, in late 2018 the Afghan Central Bank reportedly authorized certain mobile money operators to accept any letter or other form of certification from UNHCR (including the Voluntary Repatriation Form and asylum seeker and refugee certificates) to facilitate SIM registration for mobile money services as part of a cash-based intervention program.

Access to mobile money is varied for refugees across the countries studied. In Zambia, special approval was received from the Bank of Zambia and ZICTA, the telecommunications regulator, to use the proof of registration, refugee certificate and refugee ID card as valid ID for mobile wallet registration. In Nigeria, the regulatory framework is particularly progressive and accommodating.

Nigeria's mobile money framework based on a three-tier KYC/CDD regulation, the lowest level of which (Level 1) is particularly inclusive and, in theory, can accommodate the displaced (see Table 3).

Case study: Rwanda

According to the World Bank's Global Findex database, Rwanda's mobile money penetration (in terms of account ownership for 15+ years old) is 31.11%. The National Bank of Rwanda has enacted Regulation No. 08/2016 Governing the Electronic Money Issuers[72], which reiterates the core ID requirements for opening a bank account. "[Mobile Network Operators] are required to respect KYC rules prior to opening accounts — in practice a national ID card is required to register for mobile money."[73]

As such, refugees continue to face barriers to accessing mobile money. Mobile money agents from different operators are present in all camps in the country. However, while cash assistance to returnees is still based on mobile money transfers, UNHCR and WFP no longer use mobile money, but rather smart cards, for cash assistance in refugee settings due to challenges with SIM access and meeting KYC/CDD requirements.

Table 3: Tier 1 of Nigeria's Three-Tiered KYC Requirements (including Mobile Money)

	Description and characteristics	Amount / Threshold Limitation	Customer Identification requirements
Level 1	***Low Value Accounts*** i. They are subject to close monitoring by the financial institutions and less scrutiny by Bank Examiners. ii. The accounts can be opened at branches of financial institutions by the prospective customer or through banking agents. iii. No amount is required for opening of accounts iv. Such accounts cover Mobile Banking Products (issued in accordance with the CBN Regulatory Framework for Mobile Payments Services in Nigeria). ***Main Characteristics*** i. Deposits can be made by account holder and 3rd parties while withdrawal is restricted to account holder only. ii. Be linked to mobile phone accounts. iii. Operation is valid only in Nigeria. iv. Automated Teller Machine transactions are allowed. v. There is Prohibition on International Funds Transfer. vi. Accounts are strictly savings.	It is limited to a minimum single deposit amount of N20,000 and maximum cumulative balance of N200,000 at any point in time. ***Mobile Banking Products*** Level One Mobile Banking Products are Allowed: • Maximum transaction limit of N3,000 and daily limit of N30,000. • Such products are subject to the CBN Regulatory Framework for Mobile Payments Services in Nigeria.	i. Basic customer information required to be provided are: - Passport photo; - Name, Place and Date of Birth; - Gender, Address, Telephone number, etc ii. Information may be sent electronically or submitted onsite in bank's branches or agent's office iii. Evidence of the Information provided by customer or verification of same is not required.

71 Pistelli, *5 Things You Should Know About Financial Services for Refugees*: http://www.findevgateway.org/blog/2018/jun/5-things-you-should-know-about-financial-services-refugees

72 JuriAfrica, *The National Bank Regulates the Activities of Issuers of Electronic Money*: https://juriafrique.com/eng/2017/01/27/rwanda-national-bank-the-governor-enacts-new-standards-for-issuers-of-electronic-money/

73 IGC, *The Regulation of Mobile Money in Rwanda*, p.15

5. Findings

ID-related Access Barriers Remain
Despite some progress in certain jurisdictions, ID-related barriers to accessing mobile connectivity and financial services persist in many places, particularly for asylum seekers who have not yet been registered or whose registration certificate is not recognized as a legally valid form of ID for accessing mobile connectivity or financial services. The fact of the matter is this leaves millions in a particularly vulnerable position and unable to legally access services that most people take for granted.

Formal Workarounds Can Be Effective, Where Appropriate
For different reasons, displaced persons may not be in a position to acquire ID with which to access mobile and financial services. For example, there may be time constraints on a group's presence in a country that hinders access to officially recognized forms of ID (e.g. the Emergency Transit Mechanism in Niger). In cases like these, UNHCR has managed to distribute to persons of concern SIM cards registered in the organization's name (i.e. bulk registration against a legal entity identity). Likewise, where KYC/CDD rules for financial services are very restrictive or do not take into account the situation of refugees, UNHCR may need to open bank accounts in the organization's name with a sub-account in a beneficiary's name in order to facilitate cash transfers. While such formal workarounds may not be ideal from an inclusion perspective, they do provide an effective and, importantly, legal means to facilitate access in certain contexts where other means are not open.

Informal Workarounds Are Common, But Precarious and Unsustainable
On the other hand, informal workarounds are especially common across many countries. The most obvious example of such workarounds is the practice of relying on others, including locals, to register SIM cards and/or mobile money wallets on one's behalf; this practice is less common for opening bank accounts, though occurrences have been reported. Such methods are precarious because these workarounds can put displaced persons in a vulnerable position and increase their chances of being taken advantage of, for example by being forced to pay a fee demanded by the legal registrant for continued access. Moreover, longer term these workarounds are unsustainable as mobile network operators and financial service providers become more vigilant in complying with the law and as governments continue to crack down on non-compliance. As ID infrastructures are digitized and buttressed with technologies like biometrics, registering on behalf of others will prove exceedingly difficult.

Strict Requirements Risk Further Marginalizing the Vulnerable
Regardless of whether or not service providers and their agents perfectly comply with the rules at present, the existence of strict requirements in the law, such as an outright ban, risks further marginalizing or even criminalizing already vulnerable populations. It is important not to confound lax enforcement of ID requirements for activating SIM cards and mobile money wallets — a common feature across many of the countries analyzed — with the idea that the legal environment somehow facilitates access. While one might argue that weak legal compliance by service providers is overall positive for displaced persons who as a result are able to connect and gain access to mobile and financial services, this is a form of legal jeopardy that further exposes displaced persons to harm.

Tiered KYC/CDD Requirements Can Increase Access
The implementation of tiered KYC/CDD requirements in certain countries, like Nigeria, has opened up basic (i.e. low tier) access to banking and mobile money services.[74] While such risk-based measures are increasingly necessary to extend forms of access to large swathes of the population, including refugees, they are under utilized in many jurisdictions. More could be done to facilitate tiered access to mobile connectivity, bank accounts, and mobile money for the undocumented, particularly in emergency contexts.

Broadening Access to Government-Recognized ID is Key
One of the keys to addressing the challenges raised in this report is broadening displaced persons' access to forms of ID recognized by the relevant law or regulation. Considering the complexities and time scales involved in extending access to legal ID to displaced populations, both short-term and long-term options can be considered:

- Short-term measures include:
    - Improving access to UNHCR-issued credentials or those already issued to refugees and other displaced persons by host government agencies (sometimes jointly with UNHCR)
    - In cases in which national law/regulation does not already recognize these forms of ID as satisfying SIM registration and/or KYC/CDD requirements, a parallel measure would involve working with policy makers to reform the rules to legally recognize these credentials
- Longer-term, national government ID policies and practices could become more inclusive of displaced persons, i.e. by including them within national registration and ID systems. This is particularly true in States that are establishing inclusive foundational ID platforms which facilitate enrollees to have their identity authenticated for these purposes.
    - There is an emerging international trend for states to include all those present on the territory — not just citizens — in legal ID systems (i.e. population registries). In West Africa, Guinea, Côte d'Ivoire, Niger, Burkina Faso, and Benin are taking part in a World Bank-funded project which aims to achieve this goal.
    - Inclusion should be promoted within the context of an appropriate enabling environment for refugee protection, as well as with a focus on data protection, privacy, and security. The benefits and risks associated with including displaced populations in host-government foundational ID platforms must also be carefully considered; so too the risks of exclusion.

74 GSMA, *Access to Mobile Services and Proof-of-Identity*, p. 25

Legal Certainty Enables Efficient Programming
Legally certain, predictable, and consistently applied SIM registration and KYC/CDD regulations allow UNHCR and other humanitarian agencies to plan for ID needs and select suitable delivery mechanisms for connectivity and cash transfers, limiting the need to find workarounds and therefore reducing liability and exposure. It also allows service providers to comply with regulations and appropriately allocate staff and agent time. Lack of legal certainty, inconsistently applied regulations, or sudden changes in regulatory expectations can disrupt or make the delivery of humanitarian assistance inefficient.[75]

Policy Change is Possible, Often through Joint Advocacy
UNHCR and other actors work closely with policy makers and regulators to identify barriers to displaced persons' access to connectivity and financial services and strive to decrease these barriers. UNHCR leverages the presence of its field offices, as well as the expertise of partner organizations, to identify barriers to access. In some cases these barriers may have been erected inadvertently, through rash or misinformed decision making. Some governments have been amenable to rethinking such decisions. Others are open to policy reform to recognize commonly held forms of ID, particularly when the benefits to the host government can be clearly articulated.

More than Advocacy is Needed
While advocacy to expand acceptable forms of ID has been effective in some countries, more can be done. There are additional opportunities for strengthened partnerships and strategic engagement in this space, the specifics of which are elaborated in the following chapter.

75 ELAN, *Humanitarian KYC Case Studies*, p. 3

6. Recommendations

This chapter sets forth recommendations for lowering legal and regulatory barriers to displaced persons' access to mobile connectivity and financial services. It does so at different levels of intervention. The first section addresses recommendations to government stakeholders, including regulators, in host countries. The second set of recommendations is focused on actions that humanitarian and development organizations can take to reduce barriers to access across the humanitarian-development continuum.

Recommendations for Government Agencies and Regulatory Bodies
Among the various actions that host governments can pursue to reduce legal barriers to access are:

Clarify Existing Requirements
In several examined cases, the actual barrier to access was not a prohibitive law, but rather misunderstandings among stakeholders regarding the legal requirements for proving identity. This is sometimes due to the fact that service providers or their agents are unfamiliar with or uncertain about forms of ID credential held by refugees and other displaced persons.

Government agencies should clearly inform stakeholders as regards the ID credentials issued to refugees and others, how to authenticate these IDs and, where appropriate, the credentials can meet existing SIM registration and KYC requirements. Increased transparency and clarity would raise awareness and go a long way to reducing barriers to access.

Coordinate Across Government and with Humanitarian Partners
States are in the process of building and expanding their digital ID ecosystems, taking advantage of the opportunities that advances in digital technology give to provide ID and facilitate access to private and public services. Such systems have the capacity to contribute to bridging the humanitarian-development divide through ensuring the inclusion of displaced populations, along with other persons present on the territory. For this to be achieved regulatory regimes, including those which govern customers' onboarding for SIM registration, banking, and mobile money require alignment. Increased coordination across government and with humanitarian partners will be required to ensure that the displaced are included and not further left behind in these processes.

Issue ID Credentials More Expeditiously
In many countries, the law in and of itself is accommodating of refugee and other displaced groups' access to mobile connectivity and financial services. The problem in these cases is that populations lack timely access to recognized ID. While not a legal or regulatory issue *per se*, extended delays are common, which forces people to adopt informal (i.e. illegal) measures for access. A related issue concerns the validity period of documents issued by host governments to refugees and other displaced persons. Documents

that quickly expire and have to be frequently renewed can leave holders temporarily disempowered by lacking a valid ID credential, unless there are systems and processes in place that facilitate easy renewal. Where national agencies are involved in the issuance of ID credentials to displaced populations, more should be done to identify the cause of delays in providing documents to populations of concern and to mitigate these delays accordingly, as well as to assess the possibility for extended periods of validity. This could be done as part of coordinated action to ensure that host communities are also able to access recognized ID credentials.

Consider Including the Displaced in Foundational ID Platforms
Where States are developing integrated population registration systems, consideration should be given to including asylum seekers and refugees within foundational ID platforms which can be accessed by all persons present on the territory to facilitate meeting ID requirements for SIM registration and KYC/CDD. This should be accompanied by ensuring that an appropriate enabling environment is in place, including in respect of refugee protection and data protection.

Assist Authentication
By extension, government agencies, including telecommunications regulators and Central Banks, should issue specific guidance to service providers on how ID credentials issued to displaced persons can be verified as part of ID authentication for SIM registration and KYC/CDD compliance. The authority which issued the ID credential, whether that be a national government agency or a humanitarian agency such as UNHCR, could also adopt processes and systems that could assist authentication.

Implement Tiered ID Requirements
For those countries that have not already done so, the implementation of tiered ID requirements could significantly increase access to financial services including mobile money. It is also worth considering how the situation of displaced persons could be best reflected in risk-based approaches to ID requirements for SIM registration and what different tiers of mobile service would entail.

Harmonize ID Requirements
Where there are divergences in SIM registration and KYC requirements, regulators should work together to harmonize the rules, where possible. Requirements for SIM registration typically originate from a country's telecommunication authority, while KYC rules are determined by Central Banks and other financial regulators. In many countries, these bodies may not coordinate effectively, resulting in differing requirements. The effect of this lack of regulatory coordination is that customers are effectively forced to register twice for services like mobile money. GSMA recommends that SIM registration requirements be harmonized with the lowest tier of KYC requirements in a country.[76]

76 GSMA, *Access to Mobile Services and Proof-of-Identity,* p. 25

Better Manage Policy Change
When governments decide to update SIM registration and KYC/CDD rules, it is crucial to provide sufficient advance notice to all stakeholders, including humanitarian agencies, mobile network operators, financial service providers, and displaced persons themselves, so as to soften the impacts of potential disconnection or account cancellation. Managing policy change should also entail carefully considering the specific needs of displaced groups to prevent unintended consequences, like inadvertent disconnection or account revocation.

Explore Regulatory Sandboxes
Financial regulators[77] globally are exploring and experimenting with new regulatory and supervisory approaches to innovation, including financial technology. The concept of a regulatory sandbox has so far proven to be particularly appealing to the financial sector as it seeks to promote technological and data-driven innovation in a safe environment, where consumers are protected. They allow firms to test new business models and technologies under the supervision of regulators — usually with certain rules temporarily relaxed. Regulators also provide targeted guidance to sandbox participants. As of December 2018, at least 40 regulatory sandboxes were either in operation or under consideration globally, including in countries that host large numbers of displaced persons, such as Jordan, Kenya, Malaysia, Nigeria, Thailand, and Uganda.[78] In these counties, and potentially others, regulators could consider how regulatory sandboxes can be erected to facilitate innovative approaches to KYC/CDD for displaced populations in partnership with humanitarian agencies and private sector representatives.

Recommendations for UNHCR and Other Organizations
It is not just the responsibility of government to alleviate barriers to access. Actors such as UNHCR and other humanitarian and development organizations should advocate for different measures to improve displaced populations' access to connectivity and financial services.

Promote Good Practices Globally
UNHCR and like-minded agencies and organizations, potentially in collaboration with service providers, should engage policy makers internationally, regionally, and nationally to promote good practices in the areas of registration, ID, and access.

- International engagement at bodies such as the International Telecommunications Union, Financial Action Task Force, World Bank, and development banks would help to raise the profile of these issues and assist humanitarians in generating international consensus on inclusive approaches to extending access to connectivity and finance to displaced populations. In particular, advocating to the FATF for the development of refugee-specific guidance and/or recommendations would help to lessen barriers to accessing financial services for these populations. Bodies such as the Financial Inclusion Global Initiative and its Digital Identity

77 And, increasingly, telecommunications regulators; see, for example, the case of Taiwan: *5G Regulatory Sandbox Expanded* https://www.lexology.com/library/detail.aspx?g=75efca5b-069a-41e6-9aed-0ba2264a2bf3
78 Digital Financial Services Observatory, *Regulatory Sandboxes*: https://dfsobservatory.com/content/regulatory-sandboxes

Working Group could also provide an important venue for dialogue.

- There are also opportunities to engage regional FATF bodies such as Middle East and North Africa Financial Action Task Force (MENAFATF), Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), and *Groupe d'Action contre le blanchiment d'Argent en Afrique Centrale* (GABAC) on KYC/CDD-related concerns. Likewise, where they exist at regional level, organizations like the East African Communications Organisation (EACO) should be engaged to address barriers to SIM access as a matter of priority.
- At national level, it may prove beneficial to share success stories and good practices from countries in the region with the relevant regulators.

Facilitate Faster Registration/Documentation

Where possible, UNHCR should work with government counterparts to facilitate more timely registration and documentation of asylum seekers and refugees. If delays are unavoidable, UNHCR should consider advocating to government to adjust rules for SIM registration and low-tier KYC based on more accessible forms of documentation, such as credentials issued to asylum seekers. In such cases, it will be necessary properly inform stakeholders including service providers so that they are aware of the adjusted requirements.

Monitor Government ID Issuance and Policy Change

While the issuance of recognized ID credentials to populations of concern is a critical step in overcoming access barriers, in some countries UNHCR and its partners lack credible metrics in this area, making it difficult assess the ground truth as it pertains to access to ID. UNHCR can develop metrics to better monitor and measure the coverage of government-issued ID credentials to displaced populations. This will help to inform humanitarian programming and policy advocacy efforts. Moreover, better monitoring and tracking of policy developments relevant to ID, including changes to national ID frameworks, SIM registration regimes, and KYC/CDD rules, will better prepare UNHCR and other agencies to proactively identify, engage with, prepare for, and respond to these events.

Explore eKYC Mechanisms

UNHCR should also explore whether it would be possible to increase PRIMES functionality to allow service providers to undertake electronic authentication of asylum seekers and refugees' identity, including through facilitating the verification of ID credentials or by verifying biometrics by reference to PRIMES's biometric systems. Such functionality already exists for the purposes of verifying ID in certain contexts, however, it may be possible to develop and apply as a means to strengthen verification of UNHCR-issued ID credentials for SIM registration and KYC/CDD processes. This will be particularly relevant where UNHCR retains a role in refugee registration or where governments are using UNHCR's digital tools. Various technologies should be explored, including the use of Quick Response (QR) codes. In addition, UNHCR's systems could be given increased functionality to allow asylum seekers and refugees to provide 'permissioned' access to the personal ID data held in UNHCR's systems, with their identity validated through a 1-to-1 match using biometric technology. As such new processes are designed, consideration must also be given to how to facilitate verification in low connectivity environments.

Protect Data

As UNHCR continues to register refugees and other displaced persons in collaboration with host governments, as well as extending mechanisms for electronic validation of those credentials, it should do more to promote strong data protection frameworks and data protection regulatory enforcement across host States. For this, it has many willing partners such as the International Committee of the Red Cross, which is actively involved in improving data protection efforts in humanitarian contexts[79], as well as civil society organizations. Moreover, UNHCR should continue strengthening the data protection controls within its own systems.

Encourage Service Providers to Become 'Refugee Ready'

There are issues of documentation over which service providers have control. Some providers have mission statements or policies that unintentionally exclude or limit access by certain displaced populations, e.g. mission statements such as "we serve all citizens in the country" or application forms requiring a national ID card as the only acceptable form of identification, even though the law may be more permissive. UNHCR and other agencies should encourage providers to review internal policies, documentation, and eligibility and appraisal criteria for language that requires adaptation for an inclusive portfolio.[80] As an example of good practice in this area, MTN Rwanda's SIM registration form explicitly includes an option for UNHCR ID numbers, thus better informing its agents of the validity of these credentials. UNHCR and other humanitarian agencies should work with organizations such as GSMA and similar financial services trade bodies to develop awareness programs to help service providers become 'refugee ready', particularly in High Alert List for Emergency Preparedness (HALEP) countries.[81] This is an area that would greatly benefit from strong partnerships with industry organizations and could also include preparedness for increased service provision and coverage to areas where a refugee influx is expected.

79 ICRC, *Handbook on Data Protection in Humanitarian Action*: https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action

80 NpM, *Finance for Refugees*, p. 31

81 UNHCR, *High Alert List for Emergency Preparedness*: https://emergency.unhcr.org/entry/257718/high-alert-list-for-emergency-preparedness-halep



7. Final Thoughts

This final chapter reflects on emerging issues and future research relevant to legal access to connectivity and financial services for displaced populations.

Emerging Issues
Throughout the research a number of issues have emerged which require further consideration by UNHCR and other stakeholders:

- **Sanctions Compliance**: One topical issue is the question of which roles and responsibilities organizations like UNHCR should assume with respect to broader AML/CFT obligations and measures. In particular, concerns have been raised with respect to a) what UNHCR should do if and when a beneficiary's name appears on a sanctions list, b) the need to investigate potential matches, including the resolution of false positives, and c) how to work with partners such as financial service providers and other third parties to ensure that these measures are undertaken fairly and as transparently as possible.
- **Taxing Connectivity:** Another emergent regulatory trend concerns the taxation of certain forms of connectivity including social media and mobile money. In Uganda, for example, the government has implemented a tax both on social media activity (including the use of WhatsApp, Facebook and Twitter) and mobile money transactions.[82] Such measures may disproportionately and adversely impact the poor, including displaced persons.
- **Dormancy Periods:** Short dormancy periods prior to SIM deactivation can be an issue for displaced populations. This is due to the fact that humanitarian organizations rely on active lines for both engaging with community members and delivery of digital services, including transfer of cash support. Many have low levels of disposable income and as such it is not always possible to keep lines active as expenditure is prioritized on other household needs. This issue warrants further examination to note in which contexts this specifically applies and to what extent it hinders humanitarian support to refugee populations.
- **Device Whitelisting:** A related but distinct requirement to SIM registration is the growing practice of International Mobile Equipment Identity (IMEI) whitelisting. In different parts of the world, counterfeit and fraudulent devices are in circulation partly due to the lack of affordable handsets for certain users, potentially including the displaced. Largely motivated by government concerns about unpaid customs duty, IMEI registration mandates attempt to restrict the use of counterfeit/fraudulent devices by requiring users to register ID details and a phone's IMEI information on a whitelist at national level. Such policies are growing internationally, including in jurisdictions such as Azerbaijan, Bangladesh, Chile, Colombia, Ethiopia, Iran, Kenya, Lebanon, Malaysia, Nepal, Pakistan, Russia, Turkey, and Uzbekistan.[83] A legal challenge in Kenya against the Communications Authority of Kenya's approach to identifying counterfeit devices resulted in the regulator's proposed use of a Device Management System being deemed unconstitutional.[84]
- **Cryptocurrency:** The emergence of cryptocurrencies, i.e. digital assets designed to work as a medium of exchange using strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets, and their use by displaced populations, potentially presents new challenges in terms of the delivery of humanitarian aid, as well as for KYC/CDD, which ought to be further examined.
- **Demographic Considerations**: Gender, age and other demographic factors undoubtedly shape how connectivity and finance are accessed and used. Unfortunately, due to scope restrictions, this report is largely silent on these issues. These dynamics deserve dedicated focus and consideration.

Future Research
A future research agenda for legal and regulatory aspects of connectivity, financial inclusion, and digital ID could consider the following avenues, among others:

- It may be instructive to look beyond the 20 jurisdictions that formed the basis of this report to other refugee-hosting countries in which SIM registration and KYC/CDD mandates have created access barriers, especially to see whether as yet unidentified issues or practices can be identified.
- While this report has not focused on the situation of stateless persons, issues of identification and access are particularly relevant to these populations. The same methodology should be applied to stateless persons and persons at risk of statelessness who have not been forcibly displaced. Likewise, it will also be important to examine how these issues affect IDPs and host communities, for whom aspects of practice rather than legal eligibility are most relevant.

82 BBC News, *Uganda Social Media Tax to Be Reviewed*: https://www.bbc.com/news/world-africa-44798627

83 A larger number of countries have implemented IMEI blacklists in order to render stolen mobile devices useless on cellular networks. A blacklist is a better solution than a whitelist because it only places an administrative burden on problem devices, while all other devices on the network are presumed to be valid and authorized to connect. A whitelist treats all devices as potentially suspicious and represents a form of permissioned connectivity.

84 Fayo & Mukami, *CA Plan to Snoop on Mobile Devices Illegal*: https://www.businessdailyafrica.com/news/CA-plan-to-snoop-on-mobile-devices-illegal--Court/539546-4488960-144ag7az/index.html

- Where States adopt a foundational ID platform approach for all persons present on the territory, it will also be important to monitor whether refugees are actually included in these systems and what are the risks of exclusion are.
- Future research could also consider the impact of various forms of formal and informal taxation on displaced persons' access to and use of connectivity: device (IMEI) whitelisting, taxing mobile handsets, particularly at borders, and social media and mobile money tax.
- Finally, more needs to be understood about the impact of legal powers for communications and financial surveillance on the adoption and use of mobile connectivity and mobile money. For example, in Zambia it has been reported that consumers are opting to complete financial transactions via mobile money providers rather than banks partly due to perceptions of financial surveillance by the tax authorities.[85] In particular, the impacts on the displaced should be further explored.

85 Phiri, Zambians, *Wary of Taxpayer ID Rule, Opt for Mobile Money Rather Than Banks*: https://globalpress-journal.com/africa/zambia/zambians-wary-taxpayer-id-rule-opt-mobile-money-rather-banks/

References

Ahmed, Syed Ishtiaque, Md. Romael Hoque, Shion Guha, Md. Rashidujjaman Rifat, and Nicola Dell. 2017. Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems:* 906-918. https://doi.org/10.1145/3025453.3025961

Betts, Alexander, Louise Bloom, Josiah Kaplan, and Naohiko Omata. 2014. Refugee Economies: Rethinking Popular Assumptions. *University of Oxford Humanitarian Innovation Projec*t, June. https://www.rsc.ox.ac.uk/files/files-1/refugee-economies-2014.pdf

Donovan, Kevin P., and Aaron K. Martin. 2014. The Rise of African SIM Registration: The Emerging Dynamics of Regulatory Change. *First Monday* 19 (2). https://doi.org/10.5210/fm.v19i2.4351

ELAN. 2017. Humanitarian KYC Case Studies. *Electronic Cash Transfer Learning Action Network*, October. http://www.cashlearning.org/resources/library/1109-elan-humanitarian-kyc-case-studies

FATF. 2012. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. *Financial Action Task Force*, February. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

FSDA. 2018. Refugees and Their Money: Assessing the Business Case for Providing Financial Services to Refugees. *FSD Africa,* March. http://www.fsdafrica.org/wp-content/uploads/2018/03/Refugees-and-Their-Money-Assessing-the-Business-Case-for-Providing-Financial-Services-to-Refugees.pdf

Gelb, Allan, and Anna Metz. 2018. *Identification Revolution: Can Digital ID Be Harnessed for Development?* Washington, D.C.: Brookings Institution Press.

Göransson, Markus. 2018. Apping and Resilience: How Smartphones Help Syrian Refugees in Lebanon Negotiate the Precarity of Displacement. *Clingendael Institute: The Netherlands Institute of International Relations,* July. https://www.clingendael.org/sites/default/files/2018-07/PB_Mobile_phones_July_2018.pdf

GSMA. 2015. Proportional Risk-Based AML/CFT Regimes for Mobile Money: A Framework for Assessing Risk Factors and Mitigation Measures. *Mobile for Development*, August. https://www.gsma.com/mobilefordevelopment/programme/mobile-money/proportional-risk-based-amlcft-regimes-for-mobile-money-a-framework-for-assessing-risk-factors-and-mitigation-measures/

GSMA. 2016. Mandatory Registration of Prepaid SIM Cards. *GSM Association*, April. https://www.gsma.com/publicpolicy/mandatory-registration-prepaid-sim-cards

GSMA. 2017. Mobile is a Lifeline: Research from Nyarugusu Refugee Camp, Tanzania. *Mobile for Development,* July. https://www.gsma.com/mobilefordevelopment/programme/mobile-for-humanitarian-innovation/mobile-is-a-lifeline/

GSMA. 2018. Access to Mobile Services and Proof-of-Identity: Global Policy Trends, Dependencies and Risks. *Mobile for Development,* February. https://www.gsma.com/mobilefordevelopment/programme/digital-identity/access-mobile-services-proof-identity-global-policy-trends-dependencies-risks/

IGC. 2013. The Regulation of Mobile Money in Rwanda. *International Growth Centre,* August. https://www.theigc.org/wp-content/uploads/2013/08/Argent-Et-Al-2013-Working-Paper.pdf

International Committee of the Red Cross. 2017. Handbook on Data Protection in Humanitarian Action, August. https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action

International Committee of the Red Cross and Privacy International. 2018. The Humanitarian Metadata Problem: “Doing No Harm” in the Digital Era, October. https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era

Jentzsch, Nicola. 2012. Implications of Mandatory Registration of Mobile Phone Users in Africa. *Telecommunications Policy* 36 (8): 608–620. http://dx.doi.org/10.1016/j.telpol.2012.04.002

Latonero, Mark, Danielle Poole, and Jos Berens. 2018. Refugee Connectivity: A Survey of Mobile Phones, Mental Health, and Privacy at a Syrian Refugee Camp in Greece. *Harvard Humanitarian Initiative*, April. https://hhi.harvard.edu/publications/refugee-connectivity-survey-mobile-phones-mental-health-and-privacy-syrian-refugee-camp

Manby, Bronwen. 2016. Identification in the Context of Forced Displacement. *World Bank Identification for Development*, June. http://documents.worldbank.org/curated/en/375811469772770030/pdf/107276-WP-P156810-PUBLIC.pdf

Microfinanza. 2018. Assessing the Needs of Refugees for Financial and Non-Financial Services - Uganda. July. https://www.unhcr.org/publications/operations/5bd01fab4/assessing-needs-refugees-financial-non-financial-services-uganda.html

NpM. 2018. Finance for Refugees: The State of Play. *The Platform for Inclusive Finance*, August. http://www.inclusivefinanceplatform.nl/what-s-new/reports-more/conference-finance-for-refugees-making-it-work-post-conference-overview/finance-for-refugees-the-state-of-play

Shahin, Wassim. 2013. Compliance with International Regulation on AML/CFT: The case of Banks in Lebanon. *Journal of Money Laundering Control* 16 (2): 109-118. https://doi.org/10.1108/13685201311318467

UNHCR. 2014. Global Strategy for Livelihoods: A UNHCR Strategy 2014-2018. *United Nations High Commissioner for Refugees.* https://www.unhcr.org/protection/livelihoods/530f107b6/global-strategy-livelihoods.html

UNHCR. 2016. Connecting Refugees. *United Nations High Commissioner for Refugees*, September. https://www.unhcr.org/publications/operations/5770d43c4/connecting-refugees.html

Wall, Melissa, Madeline O. Campbell, and Dana Janbek. 2017. Syrian Refugees and Information Precarity. *New Media & Society* 19(2): 240–254. https://doi.org/10.1177/1461444815591967

World Bank. 2017. Forcibly Displaced: Toward a Development Approach Supporting Refugees, the Internally Displaced, and Their Hosts. *World Bank.* https://openknowledge.worldbank.org/handle/10986/25016


UNHCR
The UN Refugee Agency