

When Identification Becomes a Barrier

UNHCR Innovation Service

Global Virtual Summit on Digital Identity for Refugees

Connectivity, in particular through mobile devices, has the potential to mitigate the effects of forced displacement in important ways, including by facilitating communication and access to information, as well as by increasing social capital. Likewise, financial inclusion — that is, being able to access useful and affordable financial products and services that meet one's needs — is a key component of achieving protection and long-term solutions for refugees and other displaced persons. But access to these services is rarely straightforward for these populations of concern.

To understand why, we must first appreciate the regulatory policy context. For years, anonymous mobile connectivity was a fact of life in many jurisdictions, particularly where the prepaid model of access is predominant. However, over the past decade governments around the world have implemented legal requirements that mandate service providers to authenticate an ID proof in order for subscribers to activate and use a SIM card and thus connect. Similarly, the emergence and widespread adoption of rules for authenticating ID in order to access financial services follows from Recommendations by the Financial Action Task Force, an intergovernmental body, meant to prevent money laundering and to combat the financing of terrorism. These Recommendations are the leading source of standards for Know Your Customer (KYC)/Customer Due Diligence (CDD) measures and are intended to be implemented at the national level through legislation and other legally binding measures. National implementations stipulate the specifics of ID authentication 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.

For the vulnerable and already marginalized, the lack of a recognized ID credential constitutes a constant risk. For populations of concern, these risks are often even greater. 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 because of a lack of acceptable ID documentation may become further marginalized and disempowered.

UNHCR and its partners continue to encounter these ID-related policy challenges as part of humanitarian programming across several host countries. Strict ID requirements erect barriers to accessing mobile connectivity and impede access to financial services, including transformative innovations such as mobile money. The combined impacts of insufficiently inclusive SIM registration and KYC/CDD policies can be devastating to the undocumented and for people whose ID credentials are not recognized by host governments or service providers.

Cognizant of the need for a strong evidence base to inform appropriate action in this area, in 2018 UNHCR initiated research across 20 countries¹ on the legal and regulatory requirements that mandate that an ID be authenticated before one can access a mobile connection or financial service, including mobile money. This comparative analysis explores the state of the legal and regulatory barriers embodied by national SIM registration and KYC/CDD requirements and how they affect access to services among asylum seekers, refugees, and returnees.

¹ 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

This research² is the first of its kind to systematically understand and address the combination of these challenges and includes a number of ID-related findings and recommendations that will be of interest to the Global Virtual Summit on Digital Identity for Refugees.

The report finds that despite progress in some jurisdictions, ID-related access barriers persist across the national regulatory frameworks in most refugee-hosting countries. While formal workarounds can be effective in some cases, they do not achieve full inclusion. Informal access workarounds for accessing mobile connectivity are common and understandable in many cases, but can be precarious and are increasingly unsustainable due to advances in verification technology.

In some cases, strict ID requirements risk further marginalizing and excluding already vulnerable populations. The research finds that in a limited number of cases, tiered KYC requirements have been shown to enable access, but the key to broadening displaced persons' access to mobile connectivity and financial services is to facilitate registration into government-recognized ID systems and to enable access to government-recognized ID credentials.

The report also finds that legal certainty, predictability, and consistency around ID requirements for displaced populations can enable more effective humanitarian programming. Policy and national regulatory change has proven possible, often through joint advocacy efforts, but more can be done.

Among the report's recommendations for lowering legal and regulatory barriers to refugee and displaced persons' access to mobile connectivity and financial services are a call for governments and regulators to clarify existing ID requirements for service access, that government bodies should issue ID credentials to displaced populations more expeditiously, and that they consider the inclusion of asylum seekers and refugees in the foundational ID platforms that are being established in certain countries. Moreover, government agencies can do more to assist ID authentication, for example by issuing specific guidance to service providers on how to verify displaced persons' ID credentials. Regulators are also encouraged to implement tiered ID requirements for SIM registration and KYC/CDD, where appropriate, while harmonizing rules where possible, and better manage policy change to minimize the negative impacts on access.

The report also includes recommendations for UNHCR and other humanitarian and development organizations. Among these, it calls for increased engagement with policy makers globally to promote good practices in the areas of registration, ID, and access. Aid agencies are encouraged to work with government counterparts to facilitate faster registration and issuance of ID credentials and to monitor more closely host government issuance of credentials to better assess the 'ground truth' as it pertains to displaced populations' access to ID, as well as to monitor relevant policy changes. UNHCR is specifically encouraged to explore additional mechanisms to facilitate the ID authentication of asylum seekers and refugees that are registered by the agency (i.e. via innovative forms of eKYC), while promoting strong data protection frameworks. Finally, humanitarian and development organizations can do more to encourage service providers to become 'refugee ready' to avoid unintentional exclusion of populations of concern, particularly during emergency situations.

² "Displaced and Disconnected", Connectivity for Refugees, UNHCR Innovation Service, 2019: <https://www.unhcr.org/innovation/displaced-and-disconnected/>