Recommendation 4

Developing guidelines
for cash transfers in Somalia:

Common recipient registry

This document *Recommendation 4 – Common recipient registry* belongs to a larger set of recommendations aimed at improving mobile money cash transfer processes in Somalia. Topics covered in the set of recommendations include: MPSP service offering, automation of the cash transfers, post distribution monitoring, common recipient registry, proof of ID, and enabling ecosystem. This document focuses on a common recipient registry.

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in **Barcelona**, **Los Angeles** and **Shanghai**, as well as the **Mobile 360 Series** of regional conferences.

For more information, please visit the GSMA corporate website at **www.gsma.com**

Follow the GSMA on Twitter: **@GSMA**

The Somalia Cash Working Group (CWG) leads the inter-sectoral cash coordination mechanism and aims to improve the coordination of cash assistance, quality of implementation of cash assistance monitoring, evaluation and learning. It is co-chaired by the World Food Programme and Concern Worldwide/Somali Cash Consortium. The Financial Service Provider (FSP) workstream's objective is improving the systems and processes of humanitarian mobile money cash transfers in Somalia, benefiting programme participants by working with implementing agencies, mobile network operators, private sector and learning partners. The GSMA M4H has supported the FSP's work since 2020.

Further information on the Somalia CWG can be found here: **www.humanitarianresponse.info/en/operations/somalia/cash-activities**

GSMA Mobile for Humanitarian Innovation

The GSMA Mobile for Humanitarian Innovation programme works to accelerate the delivery and impact of digital humanitarian assistance. This will be achieved by building a learning and research agenda to inform the future of digital humanitarian response, catalysing partnerships and innovation for new digital humanitarian services, advocating for enabling policy environments, monitoring and evaluating performance, disseminating insights and profiling achievements. The programme is supported by the UK Foreign, Commonwealth & Development Office.

Learn more at **www.gsma.com/m4h** or contact us at **m4h@gsma.com**

Follow GSMA Mobile for Development on Twitter: **@GSMAm4d**

This material has been funded by UK aid from the UK government; however, the views expressed do not necessarily reflect the UK Government's official policies.

Altai Consulting partnered with Tusmo in Somalia

GSMA Mobile for Humanitarian Innovation Programme Contributors

Jaki Mebur, Market Engagement Manager

Belinda Baah, Insights Manager

Ken Okong'o, Senior Policy and Advocacy Manager

1 Current state

One of the main challenges for cash transfers in Somalia is the absence of a government ID system: most people do not have any identification document and cannot therefore prove who they are. The problem is particularly acute in South Central and Puntland. Organisations (including MPSPs when registering SIMs and opening mobile money wallets) tend to rely on a "witness system", whereby a reputed community member testifies that the person is who they claim to be.

When identifying recipients, INGOs/agencies therefore often create their own "recipient registry". They collect data (name, phone number, etc.) as well as biometric information (mostly fingerprints) when registering recipients. Each INGO/agency therefore has its own database of recipients, containing personal information and biometric data. These databases are completely independent from one another and do not communicate. In many cases these databases are a series of unconnected flat files stored in MS Excel or on servers running ODK. Such rudimentary system limits agencies' ability to interrogate and use the data, update records or link to other agencies' data systems. The only form of verification that exists is the comparison of recipients' data (name and phone number) with the MPSP customers' list prior to making a mobile money transfer. If the INGO/agency data and the MPSP data do not match, the money is not transferred, as there is no guarantee of the identity of the receiver.[1]

2 Identified challenges

Failing to identify people is a major issue, notably in terms of AML/CFT2 considerations and regulations. The absence of a government ID registry (at least in South-Central and Puntland) has led INGOs/agencies to create their own databases of recipients. However, while potentially several millions of residents have already been registered by different INGOs/agencies, there is currently no common database of the registered population. This leads to two main issues:

1. **Limited recipient verification:** During the registration process, recipients share personal information such as their name, phone number, etc. This data is captured based solely on the recipients' declarations. Wrong declarations (intentionally or not), spelling mistakes, data entry mistakes, etc. do happen, and INGOs/agencies have no way of verifying the data collected, and therefore the declarations of the respondents. The comparison of the name and phone number against the MPSP lists prior to the mobile money transfer is the only verification available for INGOs/agencies, who therefore cannot know with full confidence who they are sending funds to.
2. **Difficulty to identify and avoid duplication:** In the absence of any verification against other databases, it is very difficult to identify potential duplicates, i.e., recipients enrolled in different (but similar) programmes run by other INGOs/agencies. In a context of multiple, overlapping programmes being implemented across Somalia by different INGOs/agencies, avoiding duplication is a real challenge. Often, when registering recipients to a programme, recipients are simply asked whether they are currently registered with another cash transfer programme. In some instances deduplication does not occur between programmes within the same agencies due to the rudimentary data systems involved and lack of qualified and resourced data analysts.

> " They were asking whether we have cash vouchers from other organisations and they are telling us if you register again with us, it will interfere with your previous voucher." – **Female recipient, Doolow**

1 Mismatches between the INGO/agency data and the MPSP data can also be due to spelling mistakes, data entry mistakes, etc. These mistakes can be corrected and recipients are sometimes contacted again to verify their information. Discrepancies that cannot be solved lead to the recipient not receiving the funds, as the INGO/agency cannot know who the person is.

2 Anti-Money Laundering and Counter Terrorism Financing

The absence of a common recipient database in Somalia is due to several factors:

- **Privacy and Data protection issues:** INGOs/agencies are reluctant to share their recipient data with other entities due to privacy concerns (most INGOs/agencies do not explicitly ask their recipients at registration whether they agree for their data to be shared with third parties). There is no data protection legislation in Somalia that would allow authorities to process and store agencies' data in a trusted manner;
- **Competition between INGOs/agencies:** As INGOs/agencies compete for the same funding, some INGOs/agencies are reluctant to share recipient data on which they spent so much effort to collect;
- **Unwillingness to share:** Some INGOs/agencies are simply not willing to enter into closer cooperation with others and invest time, efforts and money for coordinating such a system, because they do not always see the wider benefits of doing so;
- **Presence of different donors:** Many donors operate in Somalia, which renders coordination on such sensitive topics more difficult. Examples of establishing common recipient databases in other countries generally occurred when a donor pushed for this to happen across several projects funded by that donor.

3 Potential solutions[3]

Despite its potential to greatly improve KYC checks and avoid duplication, establishing a common recipient database in Somalia would be a big (and potentially costly) solution. However, cost-effective solutions exist and could be localised to the Somali context to meet the needs of the humanitarian community. This would require two steps:

1. **Establishment of a common recipient registry:** INGOs/agencies could coordinate and agree on a few basic information (e.g.: name, phone number, fingerprint, programme for which the recipient is registered) to share on a common server. This approach is similar to how governments operate recipient registries in other countries. INGOs/agencies can continue to use their own system and collect additional information that they require for their own programmes but would commit to entering basic information for each of their recipients into the shared database. For data protection concerns, none of the INGOs/agencies would have direct access to this common recipient database.
2. **Implementation of e-KYC:** While INGOs/agencies could not access the common recipient database, they could however query it, with a process known as "e-KYC". Typically, after each registration session, INGOs/agencies would query the database for each recipient and look for similar already existing data in the database such as common fingerprints or phone numbers.
   - If all information (name, fingerprint, phone number) matches, this would mean that the recipient has already been registered with another programme. In this case, the INGO/agency could verify whether the recipient is eligible for enrolment in their programme or whether it violates duplication arrangements;
   - If not all information matches (a common fingerprint is found in the database but the associated name or phone number differs for example), this would mean that there is a mistake somewhere and that the recipient cannot be confidently identified. Corrective actions would need to be taken to update the information associated with this particular recipient.

3 Efforts are currently being made by the Federal Government of Somalia (FGS) with support from the World Bank Group to develop a digital ID system through the Somalia Capacity Advancement, Livelihoods and Entrepreneurship, through Digital Uplift Programme (SCALED-UP) and to implement an inter-bank payment system through the Somali Core Economic Institutions and Opportunities (SCORE) programme. The digital ID system and inter-bank payment system would improve the process significantly. However, these initiatives are expected to be developed over the long-term. The suggestions provided here concentrate on the shorter-term to enable to process to be improved in the meantime.

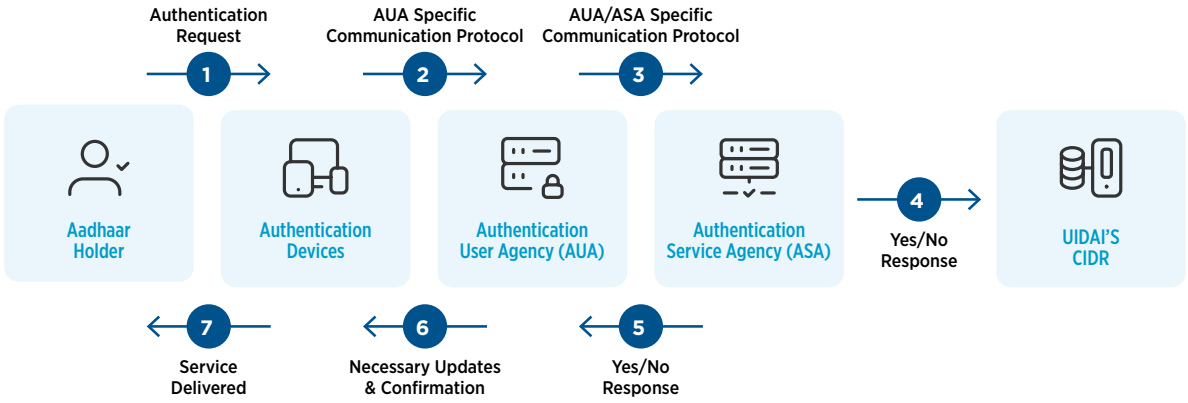
Such systems are generally managed directly by a government entity, and already exist in several contexts, including Kenya and India.4 They enable different stakeholders (financial service providers, MPSPs, administrations, etc.) to verify the identity of a person. Concretely, the person is requested to have their fingerprint scanned and provides their name, ID number or other type of information. The provider can then query the government database and verify whether the person in front of them, with this fingerprint, and claiming to be person X is indeed person X as per Government official data. Such systems have raised concerns regarding data protection and as a result, most of them only allow stakeholders to query the government database, not to access it. They are then provided with a simple "Yes/No" answer to their query (for instance, 'Does this fingerprint match this ID number?'). In some cases, the Government allows stakeholders to access limited additional information on the respondent (e.g., date of birth).

Case Study

Aadhaar authentication request in India

- Aadhaar is an initiative managed by the Government of India which aims to assign each person who resides in India a twelve digit individual identification number. It has been called by World Bank Chief Economist Paul Romer "the most sophisticated ID programme in the world".
- The programme was launched in 2009 and, as of June 2020, 1.258 billion people had been registered i.e., the vast majority of the Indian population.
- When registering on Aadhaar, individuals are requested to provide their fingerprints, iris scans, have a picture taken and provide basic demographic information.
- Authorised stakeholders, such as State agencies, can query the Aadhaar database to verify a recipient and provide them with a service they are eligible to receive. Concretely, the stakeholder requests the person to provide their Aadhaar number as well as provide their fingerprint. The Aadhaar database is then automatically queried and sends back a "Yes/No" answer indicating whether the Aadhaar number (and associated info) corresponds to the person who gave their fingerprint.

Aadhaar authentication query process



4 Overcoming the Know Your Customer hurdle: Innovative solutions for the mobile money sector, GSMA, 2019.

4 Targeted recommendations

Establishing a common recipient database and e-KYC will be one of the most difficult recommendations to implement. Looking at its benefits, it is however worth discussing such solutions, as any step towards an increased pooling of recipient data has the potential to substantially improve the current state.

Stakeholder	Recommendation	Difficulty[5]	Timeframe[6]	Cost[7]
CWG	Engage with the MoLSA led, World Bank funded, and UNICEF implemented National Registry System.	Easy	Short-term	Low
	Lead discussions with INGOs/agencies to agree on shared foundation and ownership models for such a system	Moderate	Short-term	Low
	Commission a feasibility study to determine what would be feasible within the boundaries expressed by the different stakeholders	Moderate	Medium-term	Moderate
	Lead efforts (both financing and coordination) to commission a specialised technology provider to conceptualise (based on the shared foundation) the system and develop it	High	Long-term	High
	Lead and coordinate the migration of all current recipient to the system to populate the database	High	Long-term	Moderate

5 The level of difficulty refers to the level of effort and coordination required to implement the recommendations. Recommendations with a 'low' difficulty level might only require coordination within one type of stakeholder, while those with a 'high' level may require coordination between multiple types of stakeholders.

6 The timeframe refers to how long it is assumed to take for a recommendation to be implemented. 'Short-term' recommendations are those that could be implemented within a period of three months, 'medium-term' could be implemented between three months and year, while 'long-term' recommendations could be implemented over period of more than a year.

7 The cost refers to how much each recommendation is expected to cost to implement. 'Low'-cost recommendations should require little to no cost at all to implement, 'medium'-cost recommendations would require a certain amount of investment but which could be covered by one type of stakeholder, while 'high'-cost recommendations would require significant investment from multiple types of stakeholders.

Recommendation 4

Stakeholder	Recommendation	Difficulty[5]	Timeframe[6]	Cost[7]
INGOs/ agencies	Engage in discussions lead by the CWG. Each stakeholder should share their concerns, so levels of acceptability can be determined. It is in the interest of the system to have as many INGOs/ agencies as possible to participate	Moderate	Short-term	Low
	Provide financing towards the conceptualisation and financing of the system	High	Medium-term	High
	Migrate all current recipient data to the system to populate the database	Moderate	Long-term	Moderate
	Once the system is in place, operate e-KYC on each new registered recipient, to verify their identity and avoid duplication	Moderate	Long-term	Low
MPSPs	Once a new ID system is in place, use biometrics (fingerprints) to query the database and verify new SIM or mobile money account users, thereby conducting more diligent KYC checks on customers	Moderate	Long-term	Low
Government	Support initiatives to create a common population registry: • Initiatives from INGOs/agencies • Initiatives undertaken in the framework of the larger programmes (such as Baaxnano)	Moderate	Medium-term	Moderate
	Lead on the creation of a Government national digital ID system, where registration is not based on a birth certificate but simply on the provision of biometric data to enable anyone to register, through SCALED-UP with support from the World Bank Group. The system would only aim to verify identity, not citizenship.	High	Long-term	High