UNHCR
The UN Refugee Agency

CASH ASSISTANCE AND ACCESS TO FORMAL FINANCIAL SERVICES

Information on assessing KYC and CCD regulations

INTRODUCTION

This document provides information to humanitarian practitioners on how to assess regulations relating to "Know Your Customer" (KYC) requirements, in view of delivering cash assistance to refugees and others of concern and promoting their digital financial inclusion. While the document is applicable for all forcibly displaced populations, most of the examples and learning builds on UNHCR's experience on refugees' access to financial services.

Financial inclusion of the forcibly displaced is a vital component of their protection, self-reliance and resilience.[1] To promote financial inclusion, UNHCR systematically seeks to deliver cash assistance through beneficiary-owned payment mechanisms, such as personal bank or mobile money accounts (respecting local regulations), and gives priority to open-loop systems that leverage local markets and ecosystems, rather than investing in closed-loop systems.[2] Where national regulations do not allow refugees' full-fledged access to formal financial services, UNHCR explores alternative formal means for delivering cash assistance, such as pre-paid cards or over-the-counter payments, while seeking to enhance their access to more inclusive services.[3]

By leveraging technology and mobile platforms specifically, UNHCR contributes to enhancing digital inclusion, demonstrated to bring tangible impact to the lives of refugees and others of concern.[4] The impact of COVID-19 has underlined the critical importance of access to digital and financial services.

Governments and service providers established measures to restrict usage of physical cash in preference of digital alternatives. Emergency payments have been distributed through digital channels, to encourage recipients to carry out cashless transactions.[5] Yet, refugees and other vulnerable populations, including women, are often left behind and unable to access the mainstream digital financial systems.[6]

Several factors contribute to these barriers and different population groups may face different blockages to access financial services. Refugees often do not possess identity documents from their country of origin that can be accepted as proof of identity. They can rarely register in the host State's mainstream identity systems and are instead issued alternative identity documents or credentials that are not recognised by the national regulations to access formal financial services. To date, UNHCR has successfully worked with partners to address these regulatory challenges, and, as of the end of 2020, refugees and others of concern have gained access to formal financial or digital services in some 45 countries.[7] In addition, new global guidance issued by the Financial Action Task Force (FATF) in March 2020 states that "in the case of refugees, proof of official identity may also be provided by an internationally recognised organisation with such mandate" with a reference to UNHCR, providing a potential basis for addressing the regulatory barriers and promoting refugees' access to financial services.[8]

---

[1] Financial inclusion is defined as access to and usage of quality, convenient and affordable financial products and services that meet people's needs, delivered in a safe, responsible, and sustainable manner.

[2] Closed loop system refers to a system in which the institution that issues the payment card is always the same institution that provides the acquiring infrastructure. The card or password can only be used on the acquiring infrastructure of that one institution.

[3] "Formal" in this document refers to legally recognised payments mechanisms by the relevant regulatory authority.

[4] GSMA, UNHCR (2019): "The digital lives of refugees: How displaced populations use mobile phones and what gets in the way" highlights the benefits that digital inclusion can bring to refugees.

[5] See e.g. GSMA (2020): "COVID-19 and digital humanitarian action: Trends, risks and the path forward".

[6] See e.g. IRC (2020): "COVID-19 and refugees' economic opportunities, financial services and digital inclusion".

[7] For more detail on refugees' access to different digital payments and financial services, see UNHCR (2020): "Digital payments to refugees. A pathway towards financial inclusion."

[8] Financial Action Task Force (2020): "Guidance on Digital Identity", paragraphs 54 and 56 and pages 73-75. FATF is a global intergovernmental watchdog to counter money-laundering and terrorist financing. It issues global recommendations for national regulatory bodies.

© UNHCR/Catherine Robinson

BOX 1:

Foundational and Functional Identity Systems

There are numerous types of legal identity systems, that are broadly divided into two groups. A foundational ID system is one which is primarily created to manage identity information for the general population and provide credentials that serve as proof of identity for a wide variety of public and private sector transactions and services. Common types of foundational ID systems include civil registries, universal resident or national ID systems, and population registers. A functional identification system is one created to manage identification, authentication, and authorization for a particular service or transaction, such as voting, tax administration, social programs and transfers, financial services, and more. Refugee registration systems operated by the State or UNHCR (through PRIMES, UNHCR's Population Registration and Identity Management eco-system) can provide proof of legal identity for refugees but in many contexts the identity credentials issued are not recognised to prove identity to access key services. In some operating contexts enrolment in foundational identity systems has become essential to access key services, which can create an additional barrier or opportunity for refugees, depending on the context. For example, in India, enrolment in "Aadhaar" foundational ID system and the possession of an "Aadhaar" number has been systematically required for onboarding for financial services by some providers. In Nigeria, refugees were not able to legally register SIM cards in their own name without being enrolled in the National Identity Management Commission (NIMC) foundational identity system, although this process has been simplified recently.

KYC-RELATED REGULATORY ENVIRONMENT

UNHCR's global research on access to financial services and mobile connectivity, "*Displaced and Disconnected*", has identified that one of the 'hard stops' in facilitating mobile connectivity and access to financial services for displaced populations is non-conducive regulatory environments and identity-related legal requirements.[9] For example, a refugee who cannot legally activate a mobile SIM card, open a bank account or register for a mobile money wallet in his or her own name may be further marginalized and disempowered as access to information, communication, and financial services is severely limited. The lack of legal certainty, inconsistently applied regulations, or sudden changes in regulatory expectations as regards identification can disrupt the delivery of humanitarian assistance. In some regions, other regulatory dimensions such as restrictions related to the IMEI (unique identifier of the electronic devices) may further restrict access to services.

KYC regulations are one of the principal identity related challenges that limit access to formal financial services for refugees and others of concern to UNHCR.[10] KYC regulations, which are a part of customer due diligence (CDD) measures, are designed to combat money laundering (AML), terrorist financing (CTF), and proliferation financing threats to the financial system. They refer to regulations related to identity checks that financial institutions must perform in order to comply with national AML/CFT laws and regulations, usually imposed by the relevant Central Bank. Typically, KYC checks take place when customers request to open an account or conduct certain transactions. KYC requirements are established at the national level and may vary depending, among others, on the type of customer, Financial Service Provider (FSP) (e.g. banks, mobile network operators, remittance companies, micro-finance institutions, etc.), the transfer value, the account ceiling, or the financial product itself.

BOX 2:

Note on Terminology

Customer Due Diligence (CDD) is a set of measures that financial service providers are required by regulation to undertake in certain circumstances, including when establishing business relationships. The term is found in the FATF's recommendations. CDD includes measures that FSPs must take to identify the customer and verify the customer's identity using reliable, independent source documents, data or information but also includes other steps, for example, information on the purpose and intended nature of the business relationship. Know Your Customer (KYC) is a term used to describe the identity checks that financial service providers undertake as part of CDD when onboarding the customer. KYC and CDD are often used interchangeably but regulators prefer to use the term CDD.

[9] UNHCR (2018-2021): Displaced and Disconnected. Connectivity for refugees

[10] The impact of KYC requirements is likely to be different for asylum seekers, refugees, and stateless persons compared to the nationals of the country that may have access to national ID credentials (e.g. IDPs and returnees).

Fully-fledged Bank Accounts and Financial Inclusion in Rwanda

In Rwanda, refugees have had access to full-fledged personal bank accounts since 2017, as part of the introduction of cash assistance across the camps. The Central Bank provided a waiver to use the UNHCR Proof of Registration as proxy KYC for refugees who did not yet have the formal Government-issued refugee ID, paving the way for financial inclusion.

UNHCR's and other partners' cash transfers represent a critical first step towards financial inclusion. By working through existing formal financial institutions using both banking and mobile money services, UNHCR enables recipients to access a range of financial services and products that can be used for productive purposes. In addition to receiving monthly humanitarian cash assistance for basic needs and e.g. livelihood grants, refugees also access microfinance and loans from formal microfinance institutions and social enterprises and may use services related to village savings and loans, remittances, and utility payment services. Recent assessment shows that approximately two thirds of households in refugee camps are registered with a mobile money provider and one in ten households in refugee camps have saved money on their mobile wallet account. The repayment rate (about 80%) remains high for loans. This growing trend of the usage of other financial products, in addition to cash payments, demonstrates the potential of financial inclusion to pave a sustainable way for promoting stronger livelihoods and economic inclusion of refugees and their host communities in Rwanda.

ASSESSMENT OF KYC REGULATIONS

Assessment of national KYC regulations is a key step in identifying the potential cash delivery mechanisms and can also be included in macro-economic and financial sector risk assessments. Additional resources that support such assessments include the Financial Action Task Force's Guidance on Digital Identity, on AML/CFT and financial inclusion, on Risk-Based Approach for mobile payments and for banking sector, as well as "Displaced and Disconnected" research reports and the methodology toolbox.[11]

The assessment should be undertaken prior to launching procurement of financial services, if not done already during the initial feasibility and response analysis stage. Key questions in Box 3 can guide the assessment.

See here for the questions:

Various institutions are involved in defining and enforcing KYC regulations and policies relating to refugee identification and access to services. Their roles will need to be understood and they may need to be consulted on the application of KYC requirements to refugees:

1. The host State's **Refugee Authority** will often be responsible for refugee registration and identity management, including the issuance of identity documents and related policies. The Refugee Authority often works in collaboration with UNHCR and can use UNHCR's digital tools for refugee registration known as PRIMES.

[11] FATF guidance on AML/CFT and financial inclusion; FATF Guidance on the Risk-Based Approach for mobile payments; FATF Guidance on the Risk-Based Approach for banking sector. The forthcoming methodology toolkit will be hosted on UNHCR's Displaced and Disconnected website.

It is often part of the Host State's Ministry of Interior/Home Affairs or Ministry of Foreign Affairs. In some countries, UNHCR undertakes refugee registration and identity management on behalf of the country of asylum.

2. **Central Banks** are the custodians for policies, laws and regulations related to the financial ecosystem, informed by financial intelligence units. Documentation issued by the Central Banks should hence always be reviewed when dealing with banks and other financial institutions. Banks and other FSPs may also be consulted, e.g. through bankers associations, noting however that private sector actors may perceive KYC regulations differently from the regulator.

3. **National Telecommunications Regulatory Authorities** regulate and authorise access to SIM cards and digital access more broadly, which heavily impacts and frequently prevents use of mobile money and other digital financial services. In several countries, SIM registration rules imposed by the Telecommunications Regulator are not harmonised with the KYC regulations imposed by the Central Bank. Both regulations should hence be studied when considering mobile money or other delivery mechanisms requiring a mobile device. Mobile Network Operators (MNO) or their associations may also be directly consulted, noting however that they may perceive regulations differently.

4. **Microfinance and other Non-bank Institutions** are often subject to different regulations than regular banks. These should be studied on a case-by-case basis in different countries. The national microfinance strategy or action plan may be a good start to understanding the microfinance ecosystem in the country.

5. The host State's **National Identification Authority** commonly sets and implements national policy on identification. In many countries its work is limited to citizens of the host State. However, an increasing number are also responsible for identity requirements for resident foreigners, including refugees. In countries that come from the civil law tradition it will often be part of the civil registration authority.

Understanding national policies on and digital systems for identification and the approach adopted for refugees will provide important context for the analysis.

Key Considerations

- Regulatory differences may apply to different providers (i.e. banks vs. mobile network operators vs. microfinance institutions), services (i.e. over the counter cash delivery vs. prepaid card vs. individually owned bank account vs. mobile money wallet) or transfer amounts, and national regulations may leave some room for FSPs to decide which type of ID they will accept for KYC/CDD purposes.
- Authorities increasingly put in place tiered or simplified KYC to avoid financial exclusion where the lowest tier is based on a lower level of assurance in the individuals' identity, but the product often has lower transaction limits and limited services (see below, p. 8). This approach is endorsed in the new FATF guidance, with specific reference to forcibly displaced persons and people living in situations of fragility and conflict and in the broader context of the importance of cash assistance being delivered via beneficiary owned accounts.[12]
- KYC requirements and identity credentials held are likely to be different for asylum seekers, refugees, and stateless persons than for persons of concern who are the nationals of the country (IDPs and Returnees).
- In addition to evidence of identity, FSPs may require proof of address or employment or other certificates prior to service delivery. In some cases, biometric data captured by the FSP for the purposes of identification and authentication may even be a requirement stipulated in regulations.
- Regulatory environments are evolving and there are frequent changes in regulations, in particular related to new technologies. Close coordination with financial regulators, particularly the Central Bank, is important, such as through any existing coordination mechanism.

[12] For more details, see Financial Action Task Force (2020): "Guidance on Digital Identity", paragraphs 110, 137 and 163.

- KYC rules are not always systematically enforced, and refugee-related specificities may not even be known to all FSPs or to all branches of the same FSP. This may result in FSPs proposing UNHCR payment solutions that have not been cleared by regulatory authorities and there may be geographical variations between branches.
- Data protection is key – be aware of issues related to the FSP's obligations or procedures around the disclosure of KYC information to Governments or other institutions/companies and consider with reference to the relevant organisational policies and guidelines related to data protection.[13]
- Understand the experience in the country related to KYC and Customer Due Diligence. In the event KYC regulations were relaxed, under what circumstances did this take place (what type of emergency triggered the relaxation?), how quickly, for which services, and for what length of time? Where there special provisions for refugees and others of concern?
- Are there any innovative practices/pilots taking place at the moment relating to KYC and access to financial services?

[13] See UNHCR: UNHCR Policy on the Protection of Personal Data of Persons of Concern; UNHCR Guidance on the Protection of Personal Data of Persons of Concern.

BOX 3:

Key Questions for Assessing KYC-Related Regulations

National Policies and Regulations

Financial Inclusion Policies and Regulations

- What is the host State's policy on refugees' access to financial services?
- Are refugees or other persons of concern addressed or referenced in the national financial inclusion strategy?
- What type of identity credentials/documents do the FSP require from refugees to receive cash, establish accounts or access other services? How do these vary between different services? Have risk-based approaches been implemented?
- Do these required credentials/documents reflect Central Bank's mandates or do the FSPs require additional information?
- Which Government body/bodies are responsible for refugee registration and identity management? Is UNHCR supporting the Government by undertaking these activities?
- What identity credentials/documents are refugees issued with? What type of financial services can they access with their IDs? What are the security features and what are the systems or measures in place for identity authentication?[14]
- Are there any known integrity challenges or other risks relating to refugee identification or credentials?
- Do regulations require that identity systems meet a set standard for technical robustness and level of assurance?[15]
- What are the regulatory differences that may apply for different providers, services, or transfer amounts?
- Is there a limit on the amount an individual can transact on a daily/weekly/monthly basis? Is there a limit on the amount they can hold in a mobile wallet at one time? What happens if these limits are exceeded?
- Does the country have a tiered KYC or CDD regulatory framework which allows for simplified KYC and CDD?
- Have the authorities adapted or adjusted KYC or other financial services regulations in the past in emergency situations? If so, what have these adaptations looked like?

Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CTF) Regulations/Standards

- What AML or CTF regulations are in place that dictate transaction volumes and amount limits on accounts?
- Are risk-based approaches/exceptions practiced or is there a one-size-fits-all approach to AML/CFT policy?

Data Protection

- What are the FSP's obligations or procedures around the disclosure of KYC information to the Government or other institutions/companies?

[14] For more details, see Financial Action Task Force (2020): "Guidance on Digital Identity", pages 22-24.
[15] For more details, see Financial Action Task Force (2020): "Guidance on Digital Identity", pages 47-51.

BOX 3: Continued

- What are the limitations, checks and balances enshrined in law (if any) that may allow the FSP to challenge a Government access request to disclose information about an individual, when the FSP may deem such requests as disproportionate (or putting the individual at risk)?

Regulated Financial Products and Services

Bank Accounts

- What is the local/national regulation governing KYC requirements on bank accounts?
- What types of evidence of identity and identity authentication are required for customers to open bank accounts?
- Are there additional documentation requirements for (refugee) customers that are hard to obtain (i.e. proof of income, residence)?
- What types of entities (i.e. bank branches, banking agents) can process KYC requirements and open accounts for customers?
- Are KYC rules applied consistently across FSPs' branches/agents in the country? Are these communicated to potential customers?

Digital Financial Services and E-Money Regulation, including Mobile Money[16]

- Is there a clear and separate regulation on electronic money or derivatives such as mobile money? How mature is this regulation?
- Do different (softer) rules apply to mobile money as opposed to bank accounts?
- Are there different tiers of mobile money accounts (e.g. with different savings or transactional limits per month) which may be offered to people who lack the requisite documents/credentials for KYC?
- What types of evidence of identity and identity authentication are required for customers to open mobile money accounts or access other DFS?
- Are there circulars that are still in the legislative process, or are they part of law?
- Are there specific regulations for both prepaid SIM cards (telecommunication services) and mobile money (financial services), i.e. are the two sets of rules different or harmonised?
- Are KYC rules applied consistently across mobile money agents in the country?

Multistakeholder Coordination and Engagement

- Is there a coordination mechanism in place for UNHCR, regulators/central banks/FSPs to engage on challenges related to refugees?
- Does UNHCR or other partners have any previous engagement with regulators/central banks/ financial institutions on challenges related to refugees' access to financial services?

[16] "Mobile money uses e-money which is stored value held in the accounts of users, agents, and the provider of the mobile money service. To ensure that a customer's money is available when the customer wants to redeem it, regulators typically require that the non-bank mobile money provider maintain liquid assets equal in value to the amount of money issued electronically. These funds are usually pooled in an account known as an escrow account and held by one or more banks in the name of the issuer (or in the name of a trustee appointed by the issuer)", GSMA (2019): Mobile money enabled cash aid delivery.

When Conducting the Assessments

- Conduct a desk review of publicly disseminated Central Bank and telecommunications policies (e.g. national financial inclusion and AML/CFT strategies) and regulations and those that impact digital financial services.
- Review information that may already be available within your or partner agencies (e.g. Finance, Protection/Registration, Identity Management, Supply, Cash assistance), including macro-economic and financial sector assessment of risks in the economy and financial ecosystem, including

industry and regulatory standards related to the transfer of funds, inflation, liquidity, security of financial data, AML/CTF issues, currency restrictions and other key considerations.

- Understand what communications are already ongoing between the organisation (or other humanitarian actors) and the Central Bank and the telecommunications regulator.
- Discuss with other Agencies and stakeholders in the host State that may have already conducted similar assessments and may have relevant information.
- After the desk review, consult with the Central Bank, National Telecommunications Regulatory Authority (in case of mobile money or digital financial services), private sector financial service providers, including microfinance institutions, banks and mobile network operators, the Government agency responsible for National Identity Management, and the national refugee authority in presence of the Senior Management, to corroborate information and fill any gaps.
- Include consideration of any known integrity risks relating to refugee registration and identity management (such as identity fraud, including forgery of identity documents) and mitigation measures that could be put in place prior to undertaking advocacy.
- Present, discuss and validate findings with key stakeholders in the country.

FROM ASSESSMENT TO IMPLEMENTATION

a) Where Regulatory Environment is Conducive for Financial Inclusion

In situations where financial inclusion is possible and refugees have access to formal financial services, ensure that cash assistance design and procurement systematically take into consideration and promote the potential of financial and digital inclusion.

When Procuring and Delivering Cash Assistance through an FSP:

- Ensure that procurements systematically take into consideration financial and digital inclusion potential in the selection criteria.
- Request FSPs to list their full range of financial products and services beyond the delivery of cash assistance, including savings accounts, payments, remittances or money transfers, credit and insurance, and the related KYC requirements, to better enable seamless integration of products and hence encourage the benefits of financial inclusion.
- Ensure that the protection of personal data is adequately taken into consideration and that the relevant data protection agreements of the contract are signed. Several organisations have their own templates available.
- Include (digital) financial literacy and fraud prevention training as a component of the procurement and contract with the FSPs, to ensure that refugees know that they own an account, understand the full range of services they can access and their possible cost, and can effectively use these financial services.
- Include digital literacy and skills training, as well as data literacy training to ensure that refugees have skills to use basic device functions safely, including functions relating to key digital financial services.
- Step-up awareness and socialisation on the use of the financial and digital services refugees can access.


© Astrid deVallon

- Ensure that adequate channels for feedback and complaints exist and are based around communities preferred channels of communication.
- Monitor service coverage and quality of services, to ensure recipients of cash assistance can access the services that they have the right to use.
- Monitor the use of services by refugees and their needs, to better understand the uptake of financial services and potential for further financial inclusion. This can be done through household surveys (e.g. on a sample), key informant or focus group discussions, or anonymised reports that do not infringe on recipients' privacy.
- Explore how UNHCR and other actors can promote further financial and digital inclusion, e.g. access to loans and credit, in close collaboration with key stakeholders beyond the humanitarian sphere such as development banks and institutions specialised in microfinance.

Refugee Identification and Financial Inclusion in Zambia

In Zambia, the Government's Office of the Commission of Refugees undertakes refugee registration and identity management using UNHCR's PRIMES tools. As part of refugee registration biometric data is enrolled in PRIMES. This aims to prevent individuals from being registered multiple times in the system, reducing avenues for identity fraud and misrepresentation amongst the registered population. Registered refugees are issued with a unique refugee identity number and a personal identity document. The Commissioner's Office and UNHCR service points are equipped to allow staff to verify a person's identity or eligibility for assistance. Following advocacy by UNHCR in collaboration with other key stakeholders, approval was received from the Bank of Zambia and ZICTA, the telecommunications regulator, to use the alien certificate, refugee certificate and refugee identity card as valid proof of identity to open bank and mobile money accounts. Refugees had hence gained access to formal financial services under their own name. Following the approval, UNHCR procured via a bank, the services of mobile money service providers to deliver cash-based assistance. UNHCR then partnered with MicroSave, a consulting company specialised in social, financial, and economic inclusion, to review how the shift to mobile money could be optimised to further improve cash assistance for refugees. UNHCR is giving further consideration to how electronic identity authentication, to assist FSP's KYC processes, could further strengthen identity management practices in place.

Promoting Digital Inclusion of Refugees in Uganda

In Uganda, following the arrival of over a million South Sudanese refugees since 2016, commercial connectivity services from Mobile Network Operators began to extend to hosting areas across the North West of the country. However, the regulations for telecommunications access lacked information regarding specific credentials for refugees or asylum seekers. This grey area led to inconsistent practices amongst MNOs, with lines frequently disconnected, and became an important barrier to accessing digital financial services. A technical working group, co-chaired by UNHCR and the United Nations Capital Development Fund (UNCDF), brought the GSMA, Mobile Network Operators (MNOs), Internet Service Providers (ISPs) and humanitarian response actors together to strategize on how to extend connectivity to refugees and their hosting communities, largely rural populations in remote areas of the country. The telecommunications regulator and the Office of the Prime Minister were also part of the discussion. Following collective advocacy, the working group facilitated the issuance of a directive from the Uganda Communications Commission to MNOs to open SIM card registration to those with refugee identity cards and attestation letters, breaking down a key barrier to supporting delivery of cash assistance through digital financial services, such as mobile money.

This directive provided over 600,000 refugees with a legal pathway to accessing cellular connections for the first time. The issuance of SIM cards leverages UNHCR's Biometric Identity Management System (BIMS) for eKYC and preliminary data demonstrates at least a 50% increase in mobile subscriptions amongst the adult refugee population, with up to over 500 cards issued daily.[17]

b) Where Refugees face Regulatory Barriers accessing Dormal Financial Services

Opportunities for engagement with regulatory bodies and identity issuing entities should be investigated and risks and opportunities carefully considered if KYC requirements hinder the delivery of cash assistance through formal financial services. There are different pathways for progress, depending on the context:

Promote the Recognition of Refugees' Identity Credentials

The refugee ID credentials may be issued by governments, by UNHCR or jointly by the Government and UNHCR. As is often the case, where refugees are not provided access to national foundational identity systems and refugees are registered by the Government in purpose specific, functional refugee registration systems, often using PRIMES tools. UNHCR may promote with the Government, Central Bank and National Telecommunications Agencies that the identity credentials issued to asylum seekers and refugees are sufficiently robust to prove identity for financial transactions.

Promote Refugees' Inclusion in the Host States Foundational ID Systems

This approach is likely to be a longer-term objective and will need to be subject to careful assessment and planning, including a protection assessment.

[17] See GSMA (2020): Proportionate regulation in Uganda: A gateway for refugees accessing mobile services in their own name.

UNHCR works with Governments and partners, including the World Bank's Identity for Development Programme and UNDP, to promote the inclusion of refugees within national identity systems, consistent with international legal standards and to realize SDG Target 16.9 of legal identity for all by 2030.[18] A key objective is to ensure that refugees possess government-issued or recognized identity credentials, such as identity cards and unique identity numbers that serve as proof of a person's legal or official identity and enable its authentication, including through digital means. There is a momentum to make further progress in this area as Governments increase capacity of their identification systems for their entire resident populations, often with the support of substantial international development assistance.

Explore Opportunities for Simplified KYC

Engagement with regulators about adopting simplified KYC for refugees and others of concern is particularly relevant where governments are rationalising requirements through tiered KYC to promote digital or financial inclusion and when money laundering and terrorist financing risks are low. Simplified KYC enables individuals of a specific group – such as forcibly displaced persons – to access a limited level of financial or digital services, usually with lower transaction thresholds.

When simplified KYC is applied, customers may be allowed to use nonstandard documents for access or certain requirements, such as proof of residential address, are dispensed with. The basis for any advocacy on simplified KYC approaches is hence to understand if the host State has a tiered KYC framework in place or has issued a directive related to simplified KYC. It will also be important to understand how the State manages its identity ecosystem and how the identities of refugees are managed, as well as to identify and appropriately treat any existing integrity risks relating to refugee registration and identity management prior to undertaking advocacy.

Seek a "no-objection" Letter without Amendment to Existing Regulations

The operation may seek a "no-objection" letter that will recognize the ability of refugees to access specific financial services, e.g. linked to provision of cash assistance, based on the existing identity credentials issued. This approach can also be adopted in host States where UNHCR is undertaking refugee registration on behalf of the Government, with careful consideration of existing MOUs and agreements with the host Government. Any "no-objection" letter issued would need to be shared with, and accepted, by local FSPs.

Simplifying KYC in Practice: Promoting Digital inclusion in Ghana during the Pandemic

In the context of the COVID-19 pandemic, in a directive published on 19 March 2020 the Government of Ghana outlined a series of measures to "facilitate more efficient payments and promote digital forms of payments". One measure stipulated that mobile phone subscribers should be permitted to use their existing mobile phone registration details to apply for a minimum-KYC mobile money account. This would allow all mobile phone subscribers, including refugees, to open a mobile money account using their SIM registration details. The decision to use SIM registration data was based on the data's strength and robustness, recognising potential risks that might arise from this process. It was agreed that customers registering for mobile money using SIM data could access only minimum-KYC accounts, but transaction limits were increased to take account of the restrictions on movement during lockdown. Many of the measures implemented by the Bank of Ghana have been retained by service providers during the extended crisis.[19]

[18] Sustainable Development Goal Target 16.9 states that "by 2030, provide legal identity for all, including birth registration".
[19] Financial Stability Institute (2020): Covid-19: Boon and bane for digital payments and financial inclusion.

Advocacy is more efficient if other key stakeholders promoting financial inclusion and digital inclusion are involved. These include World Bank and other Development Banks, AFI, UNCDF, ILO, UNDP, development partners, as well as global and regional standard setting bodies.[20] Private sector and regional organizations and representative bodies, including the GSMA may also have some leverage with the Government in promoting people's access to formalised means of payment. Country-level advocacy may also draw from global multi-stakeholder initiatives, such as the Coalition around the Roadmap to the Sustainable and Responsible Financial Inclusion of Forcibly Displaced Persons and UN Secretary General's Roadmap on Digital Cooperation.[21]

Further, UNHCR and partners should build a business case and engage in dialogue with financial service providers, mobile operators and other operators about refugees as an economically active and viable segments of the population and highlight their needs and rights to access financial services.[22] The lack of familiarity and misperception of displaced populations being un-bankable is still common, but new evidence is emerging. In Rwanda, a study found that refugees represented the same level of profitability for financial service providers as a typical low-income Rwandan account holder.[23] Access to financial services and financial inclusion also contributes more directly to the inclusion of poor individuals, households and small businesses in economic growth, linking to the 2030 Agenda, ensuring that no-one is left behind.

[20] Regional bodies, working with FATF, include for example ESAAMLG, MENA-FATF, GIABA, and GABAC.
[21] GIZ (2019): "Roadmap to the Sustainable and Responsible Financial Inclusion of Forcibly Displaced Persons", United Nations Office of the Secretary General's Envoy on Technology (2020): "Roadmap for Digital Cooperation".
[22] For more information, see NpM (2018): Finance for refugees: the state of play.
[23] UNHCR, AFR, FSD (2018): Refugees and their money: the business case for providing financial services to refugees.

ADDITIONAL RESOURCES

- Connectivity for Refugees: Displaced and Disconnected (UNHCR).
- Connectivity for Refugees: Displaced and Disconnected: South America (UNHCR).
- COVID-19 and refugees' economic opportunities, financial services and digital inclusion (IRC)
- Enabling Access to Mobile Services for the Forcibly Displaced: Policy and Regulatory Considerations (GSMA)
- Finance for Refugees: The State of Play (NpM, Platform for Inclusive Finance)
- Financial Inclusion of Forcibly Displaced Persons: Perspectives of Financial Regulators (AFI)
- Guidance on Digital Identity (FATF/GAFI)
- Guidelines for Financial Service Providers on Serving Refugee Populations (UNHCR & the SPTF)
- Know Your Customer and Data Protection Guidelines (UNHCR)
- Mobile Money Regulatory Index (GSMA)
- Proportionate Regulation in Uganda: A gateway for refugees accessing services in their own name (GSMA)
- Protecting Mobile Money against Financial Crimes - Global Policy Challenges and Solutions (World Bank)
- Refugees and Their Money: The Business Case for Providing Financial Services to Refugees" (UNHCR, FSD and AFR)
- Recommendations (FATF/GAFI), especially Recommendation 10
- Roadmap to the Sustainable and Responsible Financial Inclusion of Forcibly Displaced Persons
- Risk-based Customer Due Diligence – Regulatory Approaches (CGAP)
- The Delivery Guide: Scoping the Humanitarian Payments Landscape (Mercy Corps)

UNHCR project team would like to thank peer reviewers from International Rescue Committee, GSM Association, United Nations Capital Development Fund and Alliance for Financial Inclusion for their valuable comments and inputs.

UNHCR
The UN Refugee Agency

For more information, please contact:

UNHCR Global Cash Operations

Division for Resilience and Solutions, UNHCR Geneva,
hqcash@unhcr.org