Identity proofing for COVID-19 recovery: Guidance for regulators, FSPs and market facilitators

August 2020

Authors: Barry Cooper, Masiiwa Rusare, Matthew Ferreira and Lezanne Janse van Vuuren

Introduction

Customer due diligence (CDD) requirement resulting in financial exclusion in Africa. Under the updated Financial Action Task Force (FATF) recommendations (2019), Recommendation 10 requires financial institutions to adequately identify prospective clients using documents or data. It further provides examples of key identity sources, such as national identity cards. This requirement has been in place for many years across multiple iterations of the recommendations, and over the years, it has been taken by financial service providers (FSPs) and regulators to mean customers need to have a specific set of documents for CDD. This misinterpretation has directly contributed towards financial exclusion, as such requirements are both inappropriate and ineffective in many developing contexts, as individuals do not have access to such documents. For example, in sub-Saharan Africa (SSA), 17% of the adult population is excluded due to lack of documentation (Findex, 2017)[1].

Inadequate implementation of the FATF recommendations holding back economic development. Beyond implementation of recommendation 10, developing countries (particularly African countries) are struggling to implement the FATF recommendations more broadly. **Results** from the FATF mutual evaluations show that the AML-CFT frameworks in the bulk of African countries achieve a "low effectiveness" score, with no countries scoring high effectiveness for any of the criteria. This is holding back opportunities for inclusive economic development, because effective AML-CFT frameworks drive inclusive economic growth[2].

COVID-19 exacerbating already-existing challenges. COVID-19 has placed these challenges in the spotlight. Lockdown regulation and social distancing practices mean that CDD now also needs to be done remotely, which is particularly challenging because documents are normally provided and verified in person at bank or agent branches. Moreover, remote identification and verification is generally perceived to be higher risk than in-person identification and verification, and many providers have not set up their systems to facilitate remote onboarding and verification practices. As such, there is a significant risk of further financial exclusion due to COVID-19.

1 This refers to the percentage of respondents who report not having a financial institution account because they lack the documentation needed to open one, such as an identity card, a wage slip, or the like (Findex 2017).

2 See AFI and Cenfri's **inclusive integrity toolkit**, which explores how financial integrity and financial inclusion are aligned objectives and lead to inclusive economic growth.

The purpose of this note is to provide guidance to various market players regarding specific steps they can take to transition towards appropriate CDD practices that are aligned with the FATF. This will address systemic challenges in the market that have been exacerbated by COVID-19. It starts by providing an overview of the FATF's guidance relating to CDD, after which some actionable steps are outlined for different market players.

Identity proofing for COVID-19 and beyond

Utilise methodologies that are appropriately robust for the level of ML-TF risk posed by that customer. The FATF is agnostic regarding the identifiers used for CDD and particularly for the identification and verification component traditionally referred to as "KYC". It states that it should be done using "reliable, independent source documents, **data or information**" (FATF, 2019). What it does require, however, is that institutions utilise a risk-based approach when identifying and verifying[3] customers. This means that, whichever methodology is employed, it should be appropriately robust for the level of ML-TF risk posed by that customer.

Over-reliance on traditional "KYC" methodologies and analogue systems. Despite this flexibility granted by the risk-based approach, there is still significant reliance on weak analogue systems for identification and verification, which utilise human specialists and subjective assessments to confirm identity[4]. These systems are susceptible to fraud, are expensive from a business perspective and are impractical for consumers. Digital identity systems (which can perform identification and verification remotely on an ongoing basis) have been around for some time and are much more appropriate for risk-based CDD for various reasons.

- First, digital identity systems typically rely on more robust methods for identification and verification than traditional analogue systems. For example, they can use technology like biometrics to confirm identity with much higher levels of assurance than traditional systems. Where countries are still requiring documents, digital identity systems can utilise technology to check their validity more accurately than trained specialists. This is supported by the FATF, which states that "customer identification/verification measures that utilise reliable, independent **digital ID systems**, with appropriate risk-mitigation measures in place, may be standard risk, and may even be **lower risk**" (FATF Digital Guide, pg. 7).
- Second, digital identity systems conduct the identification and verification process continuously throughout the lifecycle of the account, utilising additional data collected during authentication (such as transactional data combined with GPS and IP address data) to continuously update and strengthen the identity profile. This process is referred to as ***identity proofing***, and it is critical for maintaining an up-to-date, accurate identity profile that can be assigned proportionate AML-CFT controls as per the requirements of the risk-based approach.
- Third, digital ID systems can help address financial inclusion challenges. This is because they can be utilised instead of documents for the onboarding process, or they can employ technologies to replace physical documents while achieving the same objective. They can also automate the identification process, which greatly reduces the cost and improves the

3 The risk-based method, as **defined by the FATF**, means that countries, competent authorities and financial institutions are expected to identify, assess and understand the money laundering and terrorist financing risk to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk.

4 For example, analogue systems involve clients visiting branches physically and presenting a set of documents to prove their identity. Specialists then assess the documents to check that they have not been tampered with and compare the pictures in the documents against the person to ensure the person is who they say they are.

business case of lower-income consumers. In India, for example, one **Ministry of Finance official** estimated that moving from a paper-based KYC to remote identity proofing, enabled by the **Aadhaar system**, reduced the average cost of customer verification from USD15 to USD0.50.

Transitioning towards identity proofing is essential for achieving inclusive economic development. Indeed, the concept of "KYC" is itself an outdated term that is inappropriate for the risk-based approach. KYC is a term developed by industry to refer to the practice of managing *compliance risk* by ensuring that specific documents are collected before allowing individuals to open accounts. While effective at managing compliance risk, it isn't aligned with the objectives and purpose of the FATF recommendations. While some progress has been made in recent years in transitioning towards identity proofing in Africa, COVID-19 places this need in the spotlight and highlights those countries and institutions that are still stuck in traditional, increasingly obsolete ways of undertaking CDD. For countries, fast tracking the transition to identity proofing will not only improve mutual evaluation scores but will drive achievement of aligned national objectives like financial inclusion and inclusive economic growth. For financial service providers, aligning with the standard is a matter of survival, as institutions with obsolete methodologies for customer verification will increasingly be seen as risky within international markets. Moreover, institutions can utilise identity proofing as a competitive advantage by creating a convenient experience for customers while reducing costs.

Taking a measured approach to using digital identity systems. Not all digital ID systems are *necessarily* robust or effective, and it will be important for the regulators and financial service providers (FSPs) to first assess and understand the assurance[5] levels of these systems and then utilise them accordingly. The rest of this note provides guidance to different market players on how to approach this transition effectively.

How can countries transition to remote ID proofing?

This section provides a set of actions that different markets players (regulators, FSPs and market facilitators) can take in transitioning towards utilising digital identity systems for identity proofing. Short-term actions that can be implemented immediately are first considered. These will be important for weathering the immediate crisis. Guidance is then provided on longer-term actions that can be implemented to transform the way CDD is conducted and ensure the objectives of the risk-based approach are achieved. It should be noted that the categorisation of actions into short, medium and long term is for prioritisation purposes (especially given limited resources). However, the various stakeholders could simultaneously implement the various actions (short, medium and long term).

5 Assurance levels measure the level of confidence in the reliability and independence of a digital ID system and its components (FATF, 2019).

Guidance for regulators

In the short term to medium term

1. ***Provide guidance to FSPs on the usage of digital ID systems.*** Regulators need to provide clarity on the use of different digital identity systems and ID databases available in the country that could be leveraged for remote identity proofing. For example, they can explicitly recognise certain digital ID systems as being appropriate for the CDD process by certifying them. This will enable FSPs to confidently use these systems with the knowledge that they are operating within the legal framework. It also means that FSPs don't have to do a lengthy assessment of the systems themselves, which can be expensive. These can be identity systems that have been developed either by government or by the private sector. In Singapore, for example, the Government has recognised MyInfo as an independent and reliable digital ID system to verify a customer's identity (FATF, 2020). MyInfo is a trusted identity service, which includes government-verified data retrieved from various government agencies. It allows people to access and be in control over the sharing and use of their data. In practice, people can auto-fill their government-verified personal information on public and private sector e-services on a reliable and independent channel. Currently, more than 60 financial institutions in Singapore leverage MyInfo to onboard and perform CDD on customers digitally. A challenge in Africa is that many governments may lack the funds and capacity to conduct wide assessments of ID databases. In these cases, regulators can assess and verify a few, leaving FSPs to do the assurance checks on other databases, should they wish to utilise them.
2. ***Regulators and ministries should remove legal constraints that hinder the adoption of digital ID systems.*** Another important step is for regulators to identify any legal constraints within their respective CDD frameworks that prevent remote digital identity proofing from being undertaken. The use of databases for remote identity proofing will not be possible if the CDD regulation in the country does not permit it. Where this is the case, countries need to fast-track specific legislative amendments as part of their COVID-19 relief package. Where it is possible to provide ancillary guidance, reinterpret definitions or application of regulations to enable remote identity proofing, this should be prioritised. The Monetary Authority of Singapore has issued Guidance on the "Use of MyInfo and CDD Measures for Non-Face-to-Face Business Relations". To remove regulatory barriers and promote the use of digital ID systems, this guidance stipulated that where MyInfo is used, financial institutions are not required to obtain physical documents to verify a customer's identity. In effect, this certified MyInfo by recognising it as a reliable and independent source, and it clearly removed barriers that would inhibit financial institutions from using it. A similar example exists in Thailand, whereby the central bank changed AML laws to allow a fintech operating in its regulatory sandbox to obtain and verify IDs remotely (Pearlman and Gurung, 2019).
3. ***Establish a coordinated test-and-learn environment.*** Regulators should develop a multi-stakeholder approach to (i) identifying the Digital ID system risks and opportunities relevant to their jurisdiction and (ii) assisting in developing appropriate mitigation strategies and guidance. This multi-stakeholder approach should be complemented with mechanisms to enhance dialogue and cooperation such as test-and-learn approaches. Test-and-learn approaches can be beneficial because they allow regulators to observe and evaluate the impact of an innovative product and adjust their regulation to respond to it based on the insights stemming from the evaluation (Beyers et al., 2018). To ensure that the test-and-learn environment is conducive, regulators should also monitor developments in the digital

space to generate and share best practices. The Central Bank of Egypt, for example, has acknowledged the potential of digital infrastructure to reduce barriers to customer onboarding and the potential of digital IDs to enhance risk mitigation (AFI, 2020). To cope with rapid developments in the financial technology system, the Central Bank of Egypt (CBE)'s Regulatory Sandbox acts as a live testing ground for, in this example, the safe launch of a new digital CDD solution to aid the remote onboarding of clients to mobile financial services (Muthiora, 2020). This solution was set to begin its pilot tests during January of 2020. While it is not a direct response to COVID-19, it has been intended to increase the uptake of mobile financial services amid the global pandemic and beyond.

4. ***Regulators need to align their regulatory frameworks with the FATF recommendations.*** In the short to medium term, regulators should further identify weaknesses in their regulatory frameworks, work to address these and ultimately align with the FATF. In particular, regulations should be outcomes-focused rather than inputs-focused. When regulations focus on inputs (such as the requirement of specific documents), they encourage inappropriate practices like "KYC", which do not adequately address ML-TF risk. FSPs are further limited in their ability to innovate and are constrained. If this persists in the long term, the ability of the financial sector to innovate and develop, particularly with the use of digital ID for ongoing identity proofing and ML-TF risk mitigation, will be hamstrung. South Africa's mutual evaluation is still ongoing, but it may represent a good example of a country prioritising outcomes rather than inputs for CDD. **Guidance Note 7** focuses on the achievement of AML-CFT objectives and does not strictly specify the identifiers required to be undertaken by FSPs for the CDD process[6].

In the long term

1. ***Consider developing a national or sectoral digital identity system.*** In the longer term, regulators should consider developing their own digital ID systems that can form the backbone of an ecosystem of digital services. India, for example, has developed one of the most comprehensive digital ID systems in the world. The Aadhaar system, developed in 2009, provides a unique digital ID to each citizen, and this identity number enables citizens to access a multitude of government-provided and private-sector-provided services. The identity is biometrically enabled and is explicitly integrated into the Indian payments system, allowing individuals to make remote payments, open accounts without face-to-face interactions, and receive government cash disbursements in real time (Cooper et al., 2019).

2. ***Incentivise and promote data-sharing practices.*** Regulators can consider introducing incentives to promote data sharing between FSPs as well as between FSPs and other stakeholders[7]. These could either be via directives, tax incentives or sandbox approaches to encourage stakeholders and FSPs to share identity data that is useful for the identity proofing process. This is important firstly because it could enable FSPs to conduct identity proofing remotely by utilising identity data that has already been collected and verified by another institution, and secondly because it can enable consolidation of different data pertaining to individuals, which will contribute towards formulation of national or sectoral identity initiatives. For example, in interviews with insurers in 2020, Cenfri found that some insurers in Ghana can complete the onboarding process remotely by leveraging the identity information

6 This example is explored in more detail in a **toolkit** developed by Cenfri and the Alliance for Financial Inclusion that explored methodologies for aligning financial inclusion and financial integrity.

7 This should always be done in a manner that does not violate the customer's ownership and control of their personal identification data. For example, FSPs could share data temporarily or permanently if the customer provides consent.

held at the database of MNOs with whom they have MOUs (Schlemmer et al., 2020). This is a good example of collaborating with other industry players to complete identity proofing in a way that is convenient for the customer.

3. ***Establish a data protection and privacy regime.*** A final consideration is that of privacy and data protection. A key risk with digital ID systems is the risk of data loss and the misuse of data. It is therefore the responsibility of the regulator to establish a data protection and privacy (DPP) regime in its jurisdiction, which protects the confidentiality, accuracy and integrity of the data. While this is typically assumed to be the responsibility of the data security providers, the DPP is important as a first line to reduce the risk of identity theft and cyber-attacks. The DPP is also an important first step to overcome security challenges and use rights challenges, as it creates a protective environment in which to negotiate these issues. In effect, it will increase consumer trust, thus enabling more comprehensive databases.

Digital ID systems should be governed to protect user privacy and rights. Doing so comprehensively may be difficult; however, a few key building blocks as indicated by the FATF in its digital ID guidance paper have been summarised below:

- A legal framework that describes, among other points, the purpose of the digital ID system, the means of data collection, the circumstances under which data can be shared, and how data will be corrected if inaccurate
- Institutional mandates and accountability systems that delineate the rights and responsibilities of all parties
- Oversight, monitoring and enforcing bodies that independently ensure that all parties comply with their responsibilities (These bodies should supervise the efficiency, transparency and use of digital ID systems.)
- Independent administrative and judicial authorities that have authority to provide suitable redress in the case of non-compliance or disputes

Guidance for FSPs

In the short-to-medium term

1. ***Assess the law.*** The first step is for FSPs to assess the regulatory environment and identify what they are legally required to do as part of the CDD process and what flexibility exists. This requires FSPs to understand the basic components of digital ID systems that are relevant in their regulatory environments and how they apply to required CDD processes. Potential scenarios include the following:

    - Regulation specifically requires CDD to be done in person.
    - Regulation requires specific documents and requires CDD to be done in person.
    - Regulation requires specific documents to be collected but does not require this to be done in person.
    - Regulation does not specify *how* CDD should be undertaken but requires it to be done using a risk-based approach.

    The above considerations will determine the type of digital systems FSPs could leverage and how they would use them for remote identity proofing.

2. ***Revise outdated policies and practices.*** Based on an FSP or sectoral risk assessment of current approaches, FSPs should weigh up the inherent risks and additional costs incurred by in-person physical documents and the judgement calls made by frontline staff. This should inform the alignment of their policies and practices with the FATF recommendations, national regulations and guidance, amending their internal controls to reflect best practice for remote identity proofing. For example, they could remove the assumption that non-face-to-face transactions and business relationships are always higher risk and remove outdated practices, for instance, the requirement of weak physical identifiers like proof of address.

3. ***Leverage databases and innovative technology***. FSPs should consider redeploying some of their costs related to physical document and customer scrutiny towards digital systems (where digital processes are evaluated to be more robust and dependable). This will depend on the regulatory environment as well as the type of technology and systems available in their jurisdiction. Before adopting digital identity systems for identity proofing, FSPs should conduct an assessment of the level of assurance of the relevant identity system to ensure it is appropriate for the ML-TF risks associated with the customer, product, jurisdiction, geographic reach, etc. (FATF, 2020). A few examples of the use of identity systems for remote identity proofing are provided below:

    - In South Africa, FNB leverages the Home Affairs National Identity database to undertake remote identity proofing. Users can send their identity number and a photo to FNB, which then compares this information against the Home Affairs database (including the use of facial recognition technology) to remotely proof the identity information provided. Meta-data on electronic interactions provides further assurances that strengthen the identity profile.
    - In Mexico, the voter's card and corresponding digital ID issued by the *Instituto Nacional Electoral* (INE) is being used by FSPs for remote identity proofing. The INE developed a service to allow third parties, including FSPs, to verify credentials against their database, which contains extensive information for proofing, such as fingerprint and facial biometrics. Customers can provide their INE number and corresponding biometric data remotely, and verification checks can be performed against the INE database. Users can then authenticate themselves with their biometrics when making transactions.
    - In Kenya, banks use companies like **Shufti** to onboard customers through the use of remote document proofing technology. Users send official identity documents to banks remotely, and banks employ technology to verify these documents digitally. Systems then assess, by using technology like liveness detection, whether the person is who they say they are. A risk profile is then created and updated over time to allow for alignment of account controls with risk.

4. ***Leverage officially recognised ID systems.*** An ideal situation is to use digital IDs (either developed by the State or by the private sector) that are officially recognised by government as ***appropriate*** for CDD[8]. This removes the need for the bank or FSP to do the assurance checks on the system itself. For example, Nigeria has a financial sector digital ID called the BVN (Bank Verification Number), which was developed for the purpose of robust CDD and identity management in the financial sector. Banks can utilise BVN to perform identity proofing remotely and securely without first assessing the assurance levels of the system[9].

8 This refers to the entire digital ID system being recognized as appropriate for CDD. This is different to a system which includes or utilises *official* identity documents or data.

9 More detail on BVN can be found in Cenfri and AFI's **KYC innovations** study published in 2019.

5. ***Develop a collaborative approach to CDD and ID proofing.*** Building on short-term strategies for remote proofing, FSPs should adopt a collaborative approach to CDD in the medium term. They can do this by, for example, sharing information used for identity proofing, sharing on best practices, and enabling third parties to establish identity proofing and onboarding features on their systems. These implementations have the potential to reduce costs and increase the effectiveness of CDD in the market over time. Sharing data required for identity proofing overcomes the challenges associated with opening an account for a client in isolation, which often involves data duplication, and barriers like limited and outdated data. FSPs should consider technologies such as biometrics, artificial intelligence and distributed ledger technology to make data sharing more efficient, effective and collaborative. There may, however, be impediments to this approach, such as non-disclosure agreements (NDAs) and situations where CDD confers competitive advantage. In these situations, FSPs should consider the long-term advantages of conducting CDD collaboratively, which include reduced costs of identity proofing, better transition towards open banking, and overall better ability of the financial sector to detect and combat financial crime. It is important to note that any collaborative approach must include a Data Protection and Privacy regime and should be constructed from the beginning within Privacy by Design Principles.

6. ***Considerations for financial inclusion.*** A key challenge in Africa is that many people are not part of digital ID systems with high levels of assurance or they don't have official documents that could be verified remotely. To combat this and promote financial inclusion, the FATF (2020) states that for lower-risk customers, FSPs could conduct onboarding by using digital identity systems that have lower levels of assurance for identity proofing (i.e. low levels of assurance that the person who is opening the account is who they say they are) as long as the digital ID system has sufficient authentication controls (i.e. the system has strong measures in place that prevent the account from being used by an unauthorised person). Since these accounts are opened with limited reliability for identity proofing, they must be subject to built-in AML-CFT risk mitigants, like limits on the value allowed in the account or number of transactions within a specific timeframe. As the customer uses this account, data on their transaction patterns and behaviours can be collected and analysed, which then strengthens their digital ID. This will eventually allow for the restrictions to be removed from the account. Leveraging this flexibility granted by the FATF is of utmost importance for financial inclusion and for driving inclusive growth, because people who don't have official identity from the state may have some alternative identity that could be utilised instead.

In the long term

1. ***Work with government to develop databases.*** FSPs should actively cooperate in multi-stakeholder forums to support the development of nationally recognised databases. Since FSPs have already collected much of the identity data required for the creation of digital ID databases, they could share their data with government and collaborate to assist with its development. For example, the Australian Reserve Bank in collaboration with FSPs launched the identity system "PayID" in 2018. PayID functions as a digital identity that can facilitate instant payments between any bank in Australia. The system is mutually owned by 13 institutions, which conjointly created a third-party company called New Payment Platform Australia (NPPA) in charge of maintaining and developing the platform, under a self-sustainable approach (not profit maximisation approach) (Cooper et al., 2019). Importantly, the Reserve Bank of Australia is a shareholder and was involved in the conceptualisation and development.

Although developed specifically with instant payments in mind, PayID serves as an example of the financial sector collaborating with government to create a digital financial sector identity.

Guidance for market facilitators and donors

Market facilitators and donors have a significant role to play in unlocking the above and in contributing to the development of effective digital identity systems. A few key strategies are highlighted below:

In the short to medium term

1. ***Provide support and guidance for market players.*** Market facilitators could analyse countries and/or regions and provide guidance and assistance with transitioning towards identity proofing. This could include regulatory framework reviews, identification of digital identity systems and the development of effective standards. They could also review FSPs' CDD frameworks. Donors could consider subsidising identity initiatives. For example, they could fund regional digital identity initiatives with financial sector use cases. The World Bank is a supporting regional identification programme in West Africa, called **WURI**.
2. ***Identify key leverage points for market development.*** Market facilitators should also assess markets more broadly, identify key gaps, opportunities and challenge areas, and then work towards facilitating the implementation of innovations that help to solve those challenges. For example, market facilitators could facilitate partnerships between technology providers and FSPs in order to solve specific CDD challenges identified in the market. Donors also play a role in funding case study implementations as well as funding the development and testing of ID systems that could be used for identity proofing.
3. ***Disseminate information and share best practices.*** Market facilitators act as a communicator by creating awareness of the digital systems available, their benefits and the barriers being faced when implementing them. They also ensure that new systems and mechanisms have the desired impact, particularly enabling financial and economic inclusion, as opposed to having adverse effects. Finally, market facilitators should also encourage FSPs to revise their policies and innovate by highlighting the cost of compliance, and the benefits that come with remote onboarding and digital ID such as financial inclusion and more robust AML-CFT frameworks. Donors play an essential role in funding the dissemination of appropriate information, supporting growth and developing capacities. This is specifically relevant in Africa where capacity building, especially in applying the risk-based approach, is much needed.

Conclusion

Use the crisis as an opportunity to transform CDD and make strides towards a risk-based approach. This note has provided a set of actionable interventions that different market players can take in transitioning towards the use of digital systems for ongoing identity proofing. In implementing these, it will be important for market players to recognise the broader need to view this crisis as an opportunity to transform the way CDD is approached and conducted, rather than a set of quick fixes that can address immediate concerns or provide temporary, alternative approaches to the outdated "KYC" concept. In the longer term, there is a significant need for the market to align effectively with the FATF recommendations and utilise technology appropriately to identify and verify consumers on

an ongoing basis and in a manner that aligns with risk. This will not be achieved if countries and FSPs still view this process as a “compliance” process, which adds little value to institutional or country objectives. Cenfri is currently providing further guidance and technical assistance to regulators and FSPs who are looking to approach the issue of identity proofing, but the need is great and the window for change is rapidly passing by.

Reference list

Alliance for Financial Inclusion. 2020. COVID-19 “stress tests” digital ID infrastructure. Available from: https://www.afi-global.org/news/2020/06/covid-19-stress-tests-digital-id-infrastructure.

Beyers, N., Gray, J., & Hougaard, C. 2018. Regulating for Innovation. *Cenfri*. Available from: https://cenfri.org/wp-content/uploads/2018/01/Regulating-for-innovation_Cenfri-FSDA_January-2018_updated-15-March-2018.pdf.

Cooper, B., Rusare, M., Ferreira M., Symington, J., Zahari, M.J., & Newnham, R. 2019. Inclusive Financial Integrity: A toolkit for policymakers. *AFI*. Available from: https://www.afi-global.org/sites/default/files/publications/2020-07/AFI_CENFRI_toolkit_AW_digital.pdf.

Cooper, B., Rusare, M., van der Linden, A. & Ferreira M. 2018. Biometrics and financial inclusion. *Cenfri*. Available from: https://cenfri.org/wp-content/uploads/2018/03/Biometrics-and-financial-inclusion_Cenfri-FSDA_March-2018-2.pdf.

Cooper, B., Symington, J., & Rusare, M. 2019. KYC Innovations, Financial Inclusion and Integrity in Selected AFI Member Countries. *Alliance for Financial Inclusion*. Available from: https://www.afi-global.org/sites/default/files/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries.pdf

EFInA. 2018. Access to Financial Services in Nigeria 2018 Survey. Available from: https://www.efina.org.ng/wp-content/uploads/2019/02/A2F-2018-Pre-Survey-Findings.pdf

FATF. 2020. Guidance on Digital Identity. Available from: www.fatf gafi.org/publications/documents/digital-identity-guidance.html

FinTech Egypt. 2019. The Central Bank of Egypt’s Regulatory Sandbox started its first cohort in “e-KYC” to empower the FinTech ecosystem in Egypt. Available from: https://fintech-egypt.com/news/news_details.php?id=10.

Hamilton, A. 2020. Central Bank of Egypt pilots eKYC solution for financial inclusion. Fintech Futures. Available from: https://www.fintechfutures.com/2020/01/central-bank-of-egypt-pilots-ekyc-solution-for-financial-inclusion/.

Mashingaidze, S. 2020. Zimbabwe’s ban on mobile money adds to suffering of its citizens. Business Day. Available from: https://www.businesslive.co.za/bd/opinion/2020-07-05-zimbabwes-ban-on-mobile-money-adds-to-suffering-of-its-citizens/.

Muthiora, B. 2020. Mobile money recommendations to central banks in response to COVID-19. *GSMA*. Available from: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/04/Mobile-money-recommendations-to-central-banks-in-response-to-COVID-19.pdf.

National Treasury., South African Reserve Bank. & Financial Services Board. 2007. Guidance Note 7. Available from: https://www.fic.gov.za/Documents/171002_FIC%20Guidance%20Note%2007.pdf

Kipkemboi, K., Woodsome, J., & Pisa, M. 2019. Overcoming the Know Your Customer hurdle: Innovative solutions for the mobile money sector. *GSM Association*. Available from: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Overcoming-the-KYC-hurdle-Innovative-solutions-for-the-mobile-money-sector-1.pdf

Lyman, T., Soursourian, M., De Koker, L., & Martin Meier, C. 2018. Collaborative Customer Due Diligence: New Ways Forward. *CGAP Blog Series*. Available from: https://www.cgap.org/blog/collaborative-customer-due-diligence-new-ways-forward

USAID. 2011. Being a Market Facilitator. Available from: https://www.shareweb.ch/site/EI/Documents/PSD/Tools/Resource_Box/Project%20Implementation/Team%20leading/USAID-Guide%20to%20Being%20a%20Market%20Facilitator-2011.pdf

Perlman, L. & Gurung, N. 2019. Focus Note: The Use of eKYC for Customer Identity and Verification and AML. Available at SSRN: https://ssrn.com/abstract=3370665 or http://dx.doi.org/10.2139/ssrn.3370665.

Pritchard, J. 2020. What Open Banking Is and How It Will Affect You. *The Balance*. Available from: https://www.thebalance.com/what-is-open-banking-and-how-will-it-affect-you-4173727

Schlemmer, L., Reinhard-Smit, K., & Gray, J. 2020. Never waste a crisis: How sub-Saharan African insurers are being affected by, and are responding to, COVID-19. *FSD Africa* and *Cenfri*. Available from: https://www.fsdafrica.org/wp-content/uploads/2020/07/Impact-of-COVID-19-on-insurers-10.07.201.pdf.

The World Bank. 2018. Global Identification Challenge by the Numbers. The World Bank ID4D. Available from: https://id4d.worldbank.org/global-dataset/visualization

Van Zyl, G. 2018. Opening a bank account with just a selfie – here is FNB's latest innovation. *BizNews*. Available from: https://www.biznews.com/tech/2018/05/17/opening-bank-account-selfie-fnb

About Cenfri

Cenfri is a global think-tank and non-profit enterprise that bridges the gap between insights and impact in the financial sector. Cenfri's people are driven by a vision of a world where all people live their financial lives optimally to enhance welfare and grow the economy. Its core focus is on generating insights that can inform policymakers, market players and donors who seek to unlock development outcomes through inclusive financial services and the financial sector more broadly.