cenfri

Biometrics and financial inclusion

A roadmap for implementing biometric identity systems in sub-Saharan Africa

March 2018

fsdafrica

UKaid
from the British people

Authors

Barry Cooper

Masiiwa Rusare

Albert van der Linden

Matthew Ferreira

Centre for Financial Regulation & Inclusion

Tel. +27 21 913 9510

Email: info@cenfri.org

The Vineyards Office Estate
Farm 1, Block A
99 Jip de Jager Drive
Bellville, 7530
South Africa

PO Box 5966
Tygervalley, 7535
South Africa

www.cenfri.org

Table of contents

List of figures

List of boxes

List of tables

List of abbreviations

CDD	customer due diligence
eID	electronic identity
eKYC	electronic Know-Your-Customer
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FSDA	Financial Sector Deepening Africa
FSP	financial service provider
G2P	government to person
GDPR	General Data Protection Regulations
GIABA	The Inter-Governmental Action Group against Money Laundering in West Africa
ID	Identification
ICT	information and communication technologies
ISO	International Organisation for Standardization
KYC	Know-Your-Customer
MAP	Making Access Possible
ML	money laundering
NADRA	National Database and Registration Authority
NIA	National Identification Authority
NPR	national population register
NRI	national registration institution
PoA	proof of address
RBA	Risk-Based Approach
SASSA	South African Social Security Agency
SDGs	Sustainable Development Goals
USD	United States dollar

1 Introduction

In sub-Saharan Africa (SSA), only 34% of adults have access to a bank account, compared with 51% for the Europe and Central Asia region (Findex, 2014). Financial inclusion is important for improving the livelihoods and wellbeing of individuals as well as for broader financial-sector growth, development and stability. Evidence suggests that financial-sector development (including assets, stock and bond market capitalisation, credit extension to the private sector, and liquid liabilities of financial institutions) is linked to broader economic growth (Mohan, 2006). Given the role of a functioning financial sector in uplifting livelihoods and in spurring economic growth, it is an important development agenda for Africa and SSA in particular.

The World Bank (2017) estimates that the lives of 1.1 billion people who live without proof of identity could be improved by if they gain access to digital identity. Identity can help vulnerable people to gain access to critical services, such as health services, governments grants, education and financial services such as bank accounts. Lack of legal means of identification is a problem across SSA, with varying degrees of severity. In Nigeria, 78% of the population (149 million) do not have a legal means to prove their identity, while in South Africa 12 million individuals (22%) are excluded from the formal identity system of the country (World Bank, 2017). This translates to 454 million individuals (48% of the population) across the entire SSA.

Lack of identity is a barrier to accessing a multitude of important services, particularly financial services. In response to Anti-money-laundering initiatives spearheaded by the Financial Action Task Force (FATF) (specifically Recommendation 10 on customer due diligence [CDD]), banks are required to have strong proof of identity of their customers in order to do business with them. This varies but generally includes identity documents and Proof of Address (PoA). Without such documents, consumers are excluded from accessing formal financial services. In Angola, 41% of individuals cited a lack of documents as the reason for being financially excluded, while in South Africa and Nigeria this figure was 14% and 12% respectively. Lack of identity documentation varies in its severity as a barrier to exclusion depending on the country, but overall indicates a significant problem (Findex, 2014).

Biometrics pose a possible solution to the identity problem in SSA and especially financial exclusion due to lack of identity. This is because biometrics are an inherent part of the consumer, something that the consumer does not have to carry around (such as a piece of paper or document, which is much easier to lose or damage). Moreover, biometrics are more reliable as a means of identification and significantly prevent crimes such as fraud and impersonation. This has clear benefits for the many sectors within the economy – especially the financial sector, which will be able to reduce money laundering (ML) risk through greater certainty of the identity of its customers. However, across Africa, the adoption of biometrics in identity systems has been slow and haphazard. This has led to underwhelming results and implementation of systems that are not cost-effective, scalable or interoperable.

Although a number of studies have explored the potential of biometrics in addressing identity challenges, the adoption and use of biometrics in Africa have been slow and uncoordinated at best. This is confirmed by the gap between the various approaches and the current practices on identity and biometrics. The challenge of navigating the various biometric approaches and determining the most appropriate one (among the wide range that are around) remains a key driver for slow and inappropriate adoption of biometrics approaches in Africa. However, the urgent need to address financial exclusion as well as poor financial integrity ratings (by FATF) opens up the possibility for countries to adopt biometrics approaches that promote financial inclusion, financial integrity and national development objectives in the long run. This was confirmed during Cenfri's Technical Assistance work as well as engagement with select regulators and FSPs within the GIABA and ESAAMLG regions.

Against the above background, this note seeks to understand the "biometrics journey" of countries and financial service providers (FSPs) and to help them select and adopt biometric approaches that have a lasting impact on financial inclusion, financial integrity and broader national development objectives. The first section discusses the concept of identity and the link between robust identity systems and financial inclusion. It highlights the role that lack of identity plays in facilitating financial exclusion in SSA. The second section defines biometrics, unpacking the role of biometrics in the identity space and how biometrics can be a strong identifier. The third section discusses the use cases for biometrics as well as the barriers to the successful implementation of biometric identity schemes in SSA. The final section presents a roadmap for implementing biometric identity in Africa. It is informed by the previous sections and serves as guidance to regulators, industry players and donors on how to best go about the process.

2 Identity

The concept of identity and identity systems

An identity broadly accepted as a basic human right. Article 7[1] of the Convention on the Rights of the Child states: "All children have the right to a legally registered name, officially recognised by the government. Children have the right to a nationality." This article aims to ensure that all natural persons have a legally recognised identity. Access to a legal identity is also included in the Sustainable Development Goals (SDGs). Target 9 under Goal 16[2] states: "By 2030, provide legal identity for all, including birth registration." A legally recognisable identity is key to unlock access to formal political, economic and social participation. In the absence of a verifiable identity, an individual might be denied access to basic rights and services.

The authentication of identity an increased need in an intermediated society. In ages past, human interaction was, almost exclusively, confined to those within the immediate geographical location. Social networks were limited to those within one's immediate vicinity. This phenomenon made the identification of individuals very simple. Most people had personal relations with whomever they interacted. The authentication of identification occurred through personal or social connections. This has changed. The expansion of economic circles, the need to conduct long-distance transactions and the ability to interact with those with whom we do not have personal relations have driven the need for more sophisticated identity authentication and verification mechanisms.

Identity: a collection of attributes[3]. At its core, identity is nothing more than a unique set of attributes. The attributes themselves do not have to be unique, but the combination thereof – the set – has to be unique. For example, the name John Smith is not particularly unique, but the name John Smith combined with other attributes such as a physical characteristic – a biometric – and a date of birth already increases the probability of uniqueness. It is by means of these attributes that an individual can be uniquely identified by another individual or system. Through verification of identity, the individual gains access to services. This is because verification gives the service provider, whether it be the government or a private entity, the confidence that the individual is who they claim to be.

[1] https://www.unicef.org/crc/files/Rights_overview.pdf

[2] SDG 16 concerns peace, justice and strong institutions. It forms part of the 17 SDGs, which targets universal sustainable living.

[3] http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-Identification Principles.pdf

Components of identification assertions. There are three ways through which identity can be asserted. Firstly, there is identification by something that the individual *knows*. For example, a password or a PIN that the individual memorises that can be used to gain access to a building. Secondly, there is identification by something that an individual *has*. For instance, an individual can present a physical document (such as a specific ID book), which enables access to a service. Thirdly, there is identification through something that an individual *is*, such as a physiological trait. An example of this is a biometric identifier, such as a unique fingerprint. Identity assertions that utilise the verification of a physiological trait, or biometric, are typically the most secure and the least susceptible to fraud. Authentication regimes can also use a combination of identification factors to reduce the risk of miss-identification, but often at the trade-off of efficiency (Consult Hyperion, 2017).

The concept of digital identity. At a fundamental level, digital identity is not different from any other form of identity. Similar to non-digital identity, it can be used for authentication or verification purposes. Digital identity is formed when some, or all, of an individual's identification attributes (such as a biometric) are digitally stored – for example, a card that contains a chip with machine-readable functionality. Such a card enables the user to verify their identity through a PIN or a biometric that is stored on the card. The major advantage of a digital identity is that it is designed for online identity verification mechanisms, which are typically more efficient and cost-effective than paper-based mechanisms. Today, most identification mechanisms are not digitally enabled. For instance, government-led national identity schemes are generally paper-based with no, or very little, digital functionality (Bankable Frontier Associates, 2018)

Identity system design. The design of an identity system can be centralised, decentralised or a combination of these. In centralised systems, governments issue foundational instruments[4] to its citizens, which then become their proof of identification in the National ID system. These foundational instruments serve as the basis for derivative functional identification documents[5], which are issued by other public-sector and private-sector providers. Typically, in centralised systems a single agency is responsible for both the registration of individuals in the civil registry and the

[4] Foundational identities form the basis of the ID of an individual in a country. An example of such an instrument would be a National ID card that includes a unique ID number. This card with its unique number is the strongest proof of ID that an individual can use in their country.

[5] Functional identities are created by public or private providers to enable them to identify individuals of interest uniquely. For instance, a bank has an interest in identifying account holders; therefore, it provides its customers with unique account numbers that essentially act as identification numbers at the institution. Another example is a voter registration number that is issued to voters to ensure that they only vote once in an election.

management of the national identification system. The establishment of a national population register usually occurs in a centralised identity system. This is a database of the entire population that contains demographic and socio-economic information on individuals. As key events occur in individuals' lives (marriage, for example), the NPR is updated to remain relevant. Therefore, the NPR is ideally positioned to serve as the port of call for the majority of identity-related applications. In a decentralised system, providers of foundational and functional identities maintain separate, independent identity systems. There is no hierarchy of identity systems in such a structure. The various agencies are responsible for maintaining the separate databases and ensure that it remains relevant for their specific purposes. A hybrid identity system is one that uses *both* systems in conjunction. Such a system aggregates the identity information collected by the various agencies that run their own identity schemes and constructs a unique identity for an individual (World Bank, 2017).

The make-up of an identity ecosystem. The identity ecosystem consists of various components. The starting point can be a civil registry. This is where all births and deaths are recorded. The main purpose of the civil registry is to record the existence of a nation's citizens. It often forms the foundation of an entire national identity system. The registrations in the civil register can feed into a population register. A national population register (NPR) is broader in scope than a civil register. A national ID register can, in turn, be derived from the information contained in the NPR. In most cases, only citizens that apply for a national ID token[6] are registered on the national ID register. This register contains attributes of individuals necessary for identification. For example, at this point the appropriate biometrics information can be captured and registered. In turn, this captured biometrics information can be used to verify the identity of the individual for a variety of purposes, such as customer due diligence (CDD) processes in the financial services sector. Figure 1 below illustrates the ecosystem of the Rwandan national identity system[7], but the various components of ecosystem can be configured differently.

[6] A token refers to any physical object such as an ID card or an ID book that is associated with an individual's national identity.

[7] For a more comprehensive discussion on Rwanda's national identity ecosystem, see *The Identity Ecosystem of Rwanda: A Case Study of a Performant ID System in an African Development Context* by J.J. Atick.

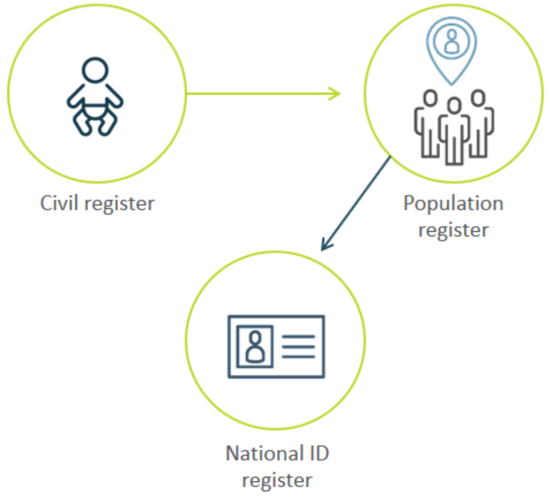

Figure 1: Rwandan national ID ecosystem

Source: World Bank, 2017

Robustness of national ID system essential for its usefulness. There is a direct link between the robustness of a national ID system and its susceptibility to fraud. If the system is easily compromised, lacks the appropriate mechanisms for accurate ID verification, or contains exemplars of inadequate quality, it will be less capable to prevent identity fraud. The utilisation of digital solutions can do much to enhance the robustness of the system. It enables the application of systems, which enhances the quality and accuracy of the information collected during the enrolment and authentication processes. It also increases the efficiency of the verification process. For instance, adopting a digital approach to the national ID system enables the usage of biometrics. A system that uses biometrics, coupled with the usage of appropriate technology, is significantly better at detecting identity fraud than a paper-based system. Committing identity fraud in a static paper-based system (particularly one that relies on functional documentation such as voter cards) is much easier because of the limitation of credential safeguards than can be included in a digital token.

The risk of identity fraud spilling through to the entire system. As mentioned earlier, the ability for an individual to identify himself/herself is key to his/her ability to participate in economic, social and political activities. Therefore, identity fraud poses serious risk to the entire economic, social and political system. If the integrity of the national ID system is compromised, the integrity of the entire system is compromised. It is therefore imperative that the robustness and security of the national ID system be prioritised, as fit for purpose.

The state of identity systems across SSA. The underpinning of a successful national identity system is universal coverage. Partial coverage implies discrimination against the segment of the population that does not have access to an identity, because of their subsequent inability to gain access to participation in formal processes. In SSA, the disparateness and limited coverage are indeed causes for concern. Figure 2 below indicates the percentage of the population of each SSA country that does not own a legal means by which to identify themselves.

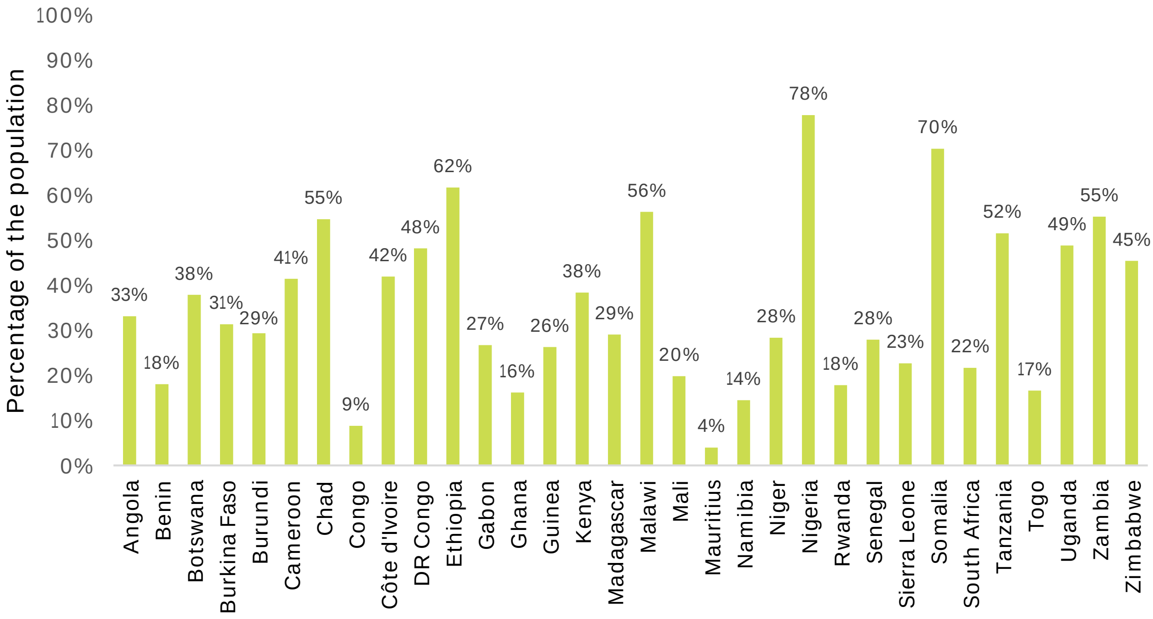

Figure 2: Percentage of population without legal proof of ID in SSA

Source: World Bank ID4D dataset, (2017)

High levels of identity exclusion across SSA. It is clear from Figure 2 above that a lot of work still needs to be done to achieve universal coverage of legal identity across SSA. In Nigeria, 78% of the population does not have a legal means to prove their identity. This amounts to 149 million individuals. Similarly, in South Africa (which has a relatively advanced national identity system), 12 million individuals (22%) are excluded from the formal identity system of the country. At the aggregate, this amounts to 454 million individuals (48% of the population) across the entire SSA. This highlights the need, and the opportunity, for a comprehensive approach to national identification systems across the continent.

The lower-income groups of societies are the most excluded. The segments of society in SSA with the lowest levels of access to documentation are the lower and lower-to-middle income groups. Figure 3 below shows the approximate distribution of individuals who do not have legal proof of identification across four income categories. The data shows that the clear majority of individuals without a legal identity is located in the low-income and lower-to-middle income groups. As a percentage, 95.4% of individuals without a legal identity are in the lower-income groups compared to 4.6% that are in higher-income groups.

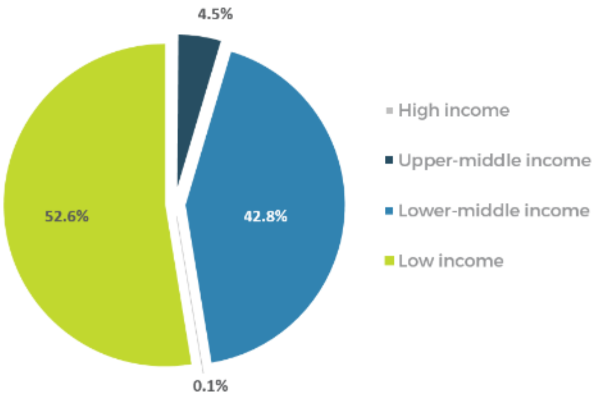

Figure 3: Income categorisation of those without a legal identity

Source: World Bank ID4D dataset, 2017

Current identity systems leaving low-income people most vulnerable. The inability of low-income people to legally prove their identity implies the existence of a significant barrier for this group to access formal services in their respective countries. For instance, the implication in South Africa is that 22% of the population will be unable to access the Social Security grant on which such a large proportion of the low-income people are so dependent. Furthermore, it also implies that the participation in the political system is often meaningfully skewed towards the higher-income population across the whole of SSA.

The CDD barrier to financial inclusion

Customer due diligence an important underpinning of financial integrity. The accurate identification of individuals and institutions that engage in the financial sector is a fundamental part of ensuring the integrity of the financial sector and the formal economy as a whole. CDD originated from the Financial Action Task Force (FATF)'s response to transnational crimes in 1989. FATF's 40 recommendations – which have since increased to 49 – focus on the supervision of the financial sector to maintain its integrity by controlling illicit financial flows. Illicit financial flows typically consist of money laundering and the financing of terrorism. Over time, the FATF measures have expanded to include measures that guide FSPs to understand and monitor the identity of their customers. It requires extensive documentation from the customer that adequately proves their identity, and it monitors the transactions of that identity.

FATF requirements regarding CDD. FATF, through its 10th recommendation, requires national jurisdictions to legislate for CDD. Financial institutions should be mandated by law to implement CDD measures. CDD measures should ensure that the FSP be confident about the identity of the individual or institution conducting the transaction by using reliable and independent source documentation to verify identity. Even after the business relationship has been established, it is imperative that ongoing CDD be conducted to ensure that the transactions be consistent with the risk profile associated with the customer FATF (2012-2018). However, through the introduction of the Risk-Based Approach (RBA) by FATF, the extent and depth to which CDD is conducted should be relative to the financial integrity risk associated with the individual and their transaction. Therefore, it is only necessary for the FSP to obtain information about the customer and understand the purpose and intended nature of the transaction to the extent to which they pose a risk to the financial sector.

Proof of address adding no meaningful identification value. FATF does not specifically require proof of address as part of the CDD process. The requirement for the client to prove their address originated in the US Banking Secrecy Act of 1970[8]. It enabled banks to triangulate references to an individual's identity in an environment that was purely paper-based. However, in a current digital environment, proof of address adds no meaningful value for financial integrity risk mitigation purposes. The whereabouts of individuals in modern, developed economies tend to be much more fluid than before. In less developed contexts, official records of residential properties or residential settlements often do not exist. For instance, in MAP Malawi[9] the proof of address component of CDD was a severe barrier to financial inclusion, as individuals could only produce sketch maps of their residential location. In such circumstances, the inclusion of proof address in CDD adds no value to ensuring the integrity of the financial system. It only serves to complicate matters and increases the burden of compliance for marginalised and rural communities. Furthermore, proof of temporary residence (such as a lease or proof of hotel booking) is widely accepted as valid proof of address for CDD purposes. In such instances, the risk mitigation of a proof of address is particularly brief.

FATF recognising that financial integrity and financial inclusion are complementary. The safeguarding of the financial sector's integrity and the provision of access to financial services are often seen as contrasting objectives. This is not the case. To have a full view of the integrity of the financial sector, all financial transactions need to be included into the formal sector. Therefore, financial inclusion is imperative to obtain financial integrity. The implication of financial exclusion is that certain financial transactions (those conducted outside of the realm of the formal financial sector) are completely unmonitored and vulnerable to abuse. Financial inclusion measures therefore enhance the reach and effectiveness of financial integrity controls (Bester, et al., 2008).

[8] The Banking Secrecy Act of 1970 is also known as the Currency and Foreign Transaction Reporting Act. It is a US law that requires financial institutions in the United States to contribute towards the Government's efforts against money laundering.

[9] MAP is a UNCDF programme conducted in partnership with FinMark Trust and Cenfri. For more information on MAP Malawi, see: https://cenfri.org/map/malawi/

Lack of identification, and accuracy of verification, a major impediment to complementarity. Financial inclusion and financial integrity can only be synergetic if the appropriate identification ecosystem is in place. It is not only the access to legal identification mechanisms that is necessary to facilitate financial inclusion and integrity, but also the quality of the mechanisms in place. If the quality of the identity mechanisms is insufficient, the verification process is compromised. This results in uncertainty on the part of the provider regarding who they are in business with, which translates into an increased risk of allowing unscrupulous individuals and transactions to enter the formal financial sector.

Therefore, a main challenge in the financial-inclusion context is the lack of reliable identification mechanisms and verification for individuals. This creates severe obstacles for CDD processes.

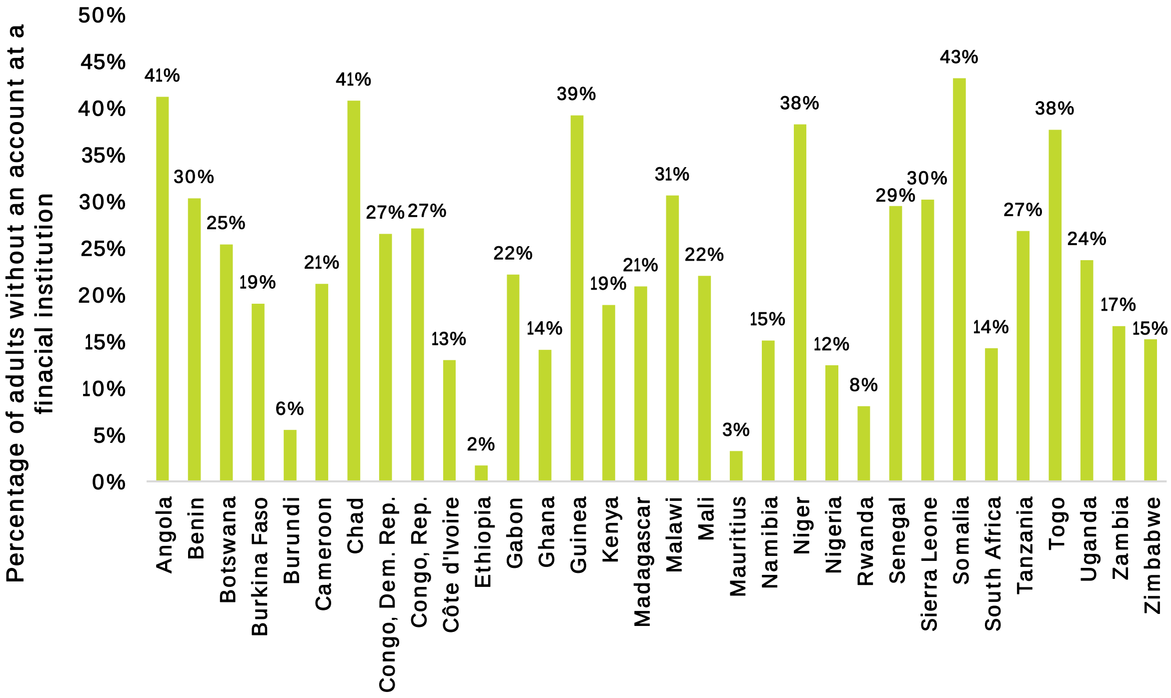

Figure 4: The percentage of financially excluded adults that cited the lack of formal identification as a reason for not having an account at a formal financial institution

Source: Findex, (2014)

Lack of access to identity documents causing financial exclusion. In the Findex 2014 survey, adults were asked why they do not currently have an account at a formal financial institution. Figure 4 above shows the results to that question for SSA. The range in results between the countries vary considerably, with only 2% of Ethiopians citing a lack of access to formal identity mechanisms as a reason for formal financial exclusion, compared to 41% of Angolans. However, individuals' inability to prove their legal identity is a major impediment to them accessing financial services. The eligibility barrier is a significant impediment to the expansion and inclusiveness of the formal financial sector. Participation in the formal financial sector is, in turn, an important driver of increasing the reach of economic development opportunities through the participation in the formal economy.

Informalisation of financial services a real risk to financial sectors in developing countries. The failure of governments to provide their population with legal means to identify themselves is forcing people to turn to the informal sector. Financial needs do not go away in the absence of formal financial services. The movement to informal also drives the illicit. Therefore, by not providing citizens with the ability to engage in the formal financial services, governments are creating an enabling environment for illicit activities. Thom *et al.* (2016) found that most of the remittance volumes and values were sent through non-regulated channels. In fact, the figures indicate a complete collapse of the formal system. Remittances flowing through formal channels decreased from USD100 million to USD22 million and then subsequently decreased to an estimated USD5 million. Total remittances flowing into the DRC has been estimated as USD9 billion. Therefore, the non-regulated sector accounts for almost all remittance flows into the DRC. The main driver of this phenomenon was the application of CDD processes by formal financial institutions to which the majority of Congolese citizens could not adhere to. Therefore, they were forced to conduct their financial lives in the informal sector due to their lack of access to legal identification. This example underlines the significant need for SSA countries to adequately develop their national identification systems. It indicates risk to the economy and financial integrity by the advancement of unregulated or supervised financial systems.

3 Biometrics

Given the difficulty associated with proving one's identity through the use of paper documents, (especially proof of address), biometrics appears to be a strong solution to this problem. This section defines biometrics and explains how biometric information is used as an identification tool. This sets the scene for understanding the value that biometrics can play in removing access barriers to financial services.

Defining biometrics. Biometrics can be defined as the science of the identification of people based on physical or behavioural traits (Jain, Flynn, & Ross, 2008). Physical traits refer to actual physiological aspects of a person, such as their fingerprints, facial features, or the sound of their voice. Behavioural traits refer to patterns of movement, place of work, activities and other behaviours that contribute to the identity of a person. Both physiological and behavioural traits can be used independently or in conjunction to identify people and are referred to as the person's biometrics. This note focuses on physical biometric identifiers, but it is important to note that behavioural biometrics can also form part of a biometric identity.

Biometrics use cases. Biometrics are used within society as an identification tool. They can be used across different sectors of society and are particularly useful because they are more resistant to fraud and are more convenient for consumers as opposed to traditional methodologies (such as passwords). Biometric information is also inherent to the consumer and can therefore provide a unique identifier that the consumer permanently carries with them.

Capturing biometric data. To use biometrics in the identification process, biometrics information needs to be stored on a database. This requires individuals to provide their biometrics. The process in which individuals provide initial readings of their biometric data is referred to as enrolment. During enrolment, biometric devices capture the biometrics information of individuals and store this on a database so that it can be referred to at a later stage (Consult Hyperion, 2017).

Storing and using biometric data. During the enrolment process, the biometrics information obtained (such as fingerprints, iris scans or facial pictures) are not stored as such but are converted into mathematical files that are known as biometrics *templates* (Thakkar, 2017). These biometrics templates, rather than the biometrics themselves, serve as digital representations of the biometrics of a person, and they are used in the verification process to confirm that the biometrics information being provided matches with the stored template.

> "A biometric template, or profile, is a statistical analysis of the measurement, resulting in a specific reduced data set that can be used to represent the physical characteristics or features of an individual. It is important to emphasise that, for example, a fingerprint template is not the same as a fingerprint" (Consult Hyperion, 2017).

Identification versus verification. Within the broader context of identity, biometrics are used in two ways in particular: *identification* and *verification*. These two concepts are compared in the figure below.

Identification

In biometrics, identification occurs when one tries to establish *who* someone is. In practice, a consumer would provide their biometric information, and this information would be checked against a database to see whether it matches any profiles provided. This is referred to as conducting a “one-to-many comparison” (1:N).

Identification asks the question “*who is this person*?

Verification

Verification occurs when trying to establish whether a person is who they say they are. This is known as a 1:1 comparison. In practice, a consumer provides their biometric information as well as a claimed identity. Instead of searching an entire database to see whether there are matches (as in identification), the database searches for the claimed identity and compares it against the provided biometrics.

Verification asks the question “is this person who they claim to be?”

Figure 4: Identification and verification in biometrics

Source: Consult, 2017

This process of verification (1:1) is less time-consuming and requires less computing power than 1:N, as it only involves checking the *claimed identity* on the database as opposed to checking the entire database for a match. Verification can be used when conducting financial transactions to ensure the legitimacy of the person that is conducting the transaction (that the person is who they say they are). Verification is typically used to ensure that multiple people do not use the same identity, by confirming that their biometrics match the claimed identity (Jain et al., 2008)

Reliability and authenticity of biometric systems. Biometrics are prone to errors that affect the reliability of the system. These errors include: failure to enrol, false rejections and false acceptances. Failure to enrol occurs when the biometric hardware cannot capture data of an acceptable quality to create a template. For example, if an individual has very degraded fingerprints, a biometrics device may not be able to find sufficient minutiae in the fingerprints to create a template. False acceptances and rejections exist because of the way in which biometric identity systems assert matches during the identification and verification process. Indeed, no two biometric images are identical. Even the same fingerprint will produce slightly different readings each time they are assessed by a device. As such, biometric systems do not require provided templates to be *identical* to stored templates, they require them to be *very similar*. The degree of similarity required to assert a match varies depending on the system, and this is referred to as the threshold (Jain et al. 2008). If a person submits their biometrics and they get rejected despite being the person they claim to be, this is known as a false rejection, and it occurs because the provided biometric does not match closely enough with the stored template. If a person submits a biometric and is matched with the person they claim to be (despite not actually being this person) then a false acceptance has occurred. This happens when the biometric provided matches closely enough to the stored template to pass – even though the provided template was provided by someone other than the owner of the template on the database. The threshold for acceptance/rejection therefore determines the degree of authenticity of the system. The threshold should not be set so high that too many false rejections occur, but it also should not be low enough to allow significant false acceptances (Jain et al., 2008).

The following box is a discussion regarding the various types of biometrics that can be measured and converted into biometric templates for identification purposes. This discussion is not meant to be exhaustive and draws from papers that have already covered this in greater detail, such as Consult Hyperion (2017), Jain et al. (2008) and (Saini & Rana, 2014).

Box 1: Types of biometrics that can be used for identification purposes

Fingerprint

The fingerprint is one of the most common biometrics that is captured for identification purposes. It involves the capture of fingerprint images, involving either all ten fingers, two thumbs, five fingers or some other combination, with the capture of more of the person's fingerprints generally increasing the accuracy of the biometric template. Although it is widely used, fingerprint biometrics can encounter issues. Injuries, traumas, wounds or cuts can make the fingerprint-reading unidentifiable, while some fingerprints are very faint and therefore difficult to capture properly, causing failure to enrol.

Facial recognition

Facial recognition involves an evaluation of facial features and creation of a profile based on those facial features. The user can then verify their identity by simply presenting their face to facial analysis systems. The system is advantageous as it can verify people within a crown and it doesn't require any physical contact. However, it requires good lighting, is relatively expensive and can have a high error rate if facial expressions vary during tests.

Finger vein and palm vein

This type of biometric involves analysis of the physical and behavioural features of the veins of the finger and/or palm. It is highly accurate and cannot be faked, but it is expensive and inefficient for large-scale adoption.

Iris

Iris biometrics involve the scanning of the iris of the person and creation of a template based on iris features. The iris possesses a unique structure that is shaped by 10 months of age. It is highly accurate because genetically similar people still have different iris biometrics. It doesn't require any contact, has a high level of security and a high processing time. However, it is susceptible to errors due to distance from scanner, reflections from spectacles, and eye lashes. The equipment is also expensive.

Voice

Voice biometrics comprise numerical representation of the sound, rhythm and pattern of an individual's voice (voiceprint). This technique helps those people who have difficulty in using their hands. It is also easy to use, quick to process identities and user-friendly. In terms of issues, external noises can affect the accuracy of the verification process, voices can be faked and hacked, and voice files are quite large (thus requiring a large database for storing).

Hand geometry

Hand geometry biometrics involve the analysis of the characteristics of the hand, such as finger length and width, distance between finger joints, and bone structure. Spreading of germs during the onboard process and the changing structure of the hands are possible issues with hand geometry biometrics. The hand geometry also changes over time. Hand geometry is considered to be relatively accurate.

Keystroke

Keystroke technologies capture the manner or rhythm in which users type characters on keyboards. Varied typing styles can cause false rejections, which makes this technique less accurate than others.

Source: Consult Hyperion (2017), Jain et al. (2008) and (Saini & Rana, 2014)

4 Biometric considerations

Use cases

There are multiple use cases for biometrics within society, and these vary depending on the type of institution and the specific needs within that sector. Although this note focuses on the role that biometrics can play in shaping the financial sector, it is important to also understand the broader use cases for biometrics within society, as the efficiency and affordability of biometric systems depend on the ability to access multiple use cases. Therefore, this sub-section will cover the use cases for biometrics across the public and private sector within the broader society, as well as the financial sector. The findings are based on key stakeholder interviews and desktop research.

Increasing the efficiency of the CDD process. The customer due diligence (CDD) process is costly for banks, as it involves the compilation and assessment of a multitude of documents related to clients. The analysis and maintenance of these documents in assuring the identity of clients can be cumbersome and costly, due to the time and labour associated with doing so (Iritech, 2016). Biometrics have the potential to remove this barrier by providing certainty of the identity of the person who wants to make use of financial products and services – by means of a simple fingerprint, facial scan or iris recognition. There is also potential to access centrally held and verified information such as a financial identity documentation at industry or national levels. This eliminates the requirement for individual service providers to replicate and verify the individual data.

By only requiring the biometrics of an individual, the cost associated with verifying their identity is significantly reduced and the process becomes more efficient. Moreover, the process is simplified for consumers, who can use their biometrics during the onboarding procedure instead of requiring multiple documents. By enhancing efficiency in the CDD process from the provider and consumer perspective, access to, and uptake of, financial services are expected to increase significantly. In Kenya, for example, The Kenyan National Identity Authority maintains a database of the identities of its population, and this identity includes biometric information. Many Kenyan banks are able to identify their customers by scanning their biometrics and linking to the National Identification Database to verify the identity of the individual. By providing a simple biometric, banks can cross-check that a client's assumed identity matches with their digital identity on a database. This is highly advantageous and decreases onboarding and CDD costs for banks (stakeholder interviews, 2017/2018).

Decreasing institutional risk for banks.
Using biometrics to verify the identity of clients not only decreases costs for FSPs; it also decreases risks. The usefulness of biometrics in providing certainty of the identity of customers has an effect on the ability of banks to grow and establish important relationships with other banks. If banks are able to identify their customers with greater certainty, their compliance risks are reduced. More specifically, the enhanced ability to identify clients with certainty means that banks have a much better understanding of the nature and risk profile of their clients, which means they are less likely to facilitate money laundering unknowingly and less likely to incur compliance penalties. Improved frameworks for risk assessments and reduced compliance-related risks are likely to improve the reputation of local banks, therefore facilitating greater correspondent banking relationships. This plays an important role in facilitating the development of the banking sector as a whole – which relies on established networks and connections to other banks[10]. For example, in Nigeria the telecommunications company MTN was fined over USD5 billion because it apparently aided the terrorist group *Boko Haram* as a result of lax implementation of CDD procedures (Allison, 2016). MTN has since introduced biometrics in its customer identification procedure in Nigeria.

Facilitating the extension of credit.
The ability to confirm identities with greater confidence leads to a decrease in impersonation fraud. In the financial sector, lenders can operate with more certainty and confidence when they have high-quality information about their borrowers. Biometrics enable FSPs to be more certain of the identity of their clients and to access important information regarding their repayment behaviour, should this information be linked to their financial or national ID. For example, the Central Bank of Uganda implemented a biometrics-based finance card known as the "financial card system", and by 2009, bank branches in Uganda had the infrastructure to register consumers biometrically and issue a banking identity. This biometrics card was linked to the Ugandan credit bureau, which provided information regarding the repayment behaviour of the individuals. This enabled lenders to have access to repayment information of their clients and potential clients and provided an ecosystem for lenders to act with more certainty (International Financial Corporation, 2012). This has the ultimate effect of facilitating the extension of credit into the economy, thus increasing

[10] Establishing greater relationships between banks should also drive down the cost of international payments and remittances, ultimately facilitating economic growth and development.

access to financial services, but also stimulating economic growth.

Enhancing security and convenience for consumers. Using biometrics across the financial services industry helps to reduce fraud and increase security. Rather than using PIN codes to make payments or draw money at ATMs, consumers can instead use their biometrics to verify their identity, such as a fingerprint or facial scan. This removes the need to remember passwords, which increases convenience for consumers but also increases security, as payments or withdrawals cannot be made by anyone other than the account owner. Unfortunately, the uptake of these types of services is relatively low, as biometrically authenticated transactions require devices that can read and process biometrics data, and these devices are not widely installed across Africa. In South Africa, Mastercard recently tested a new card that has fingerprint scanning technology (Mastercard, 2017). These cards are expected to be rolled out in South Africa in the near future, and they will give customers greater security and resilience to the effects of card theft. In Kenya, some banks are already using biometric ATM solutions that allow customers to draw money and access ATMs simply by using their fingerprint, which links to the national identity database. However, this type of technology has not yet been used extensively and is still in its early stages of uptake (stakeholder interviews, 2017/2018) Perhaps one of the most compelling use cases is the Aadhaar programme in India, whereby consumers are able to provide their unique identification number (which is biometrically linked to their fingerprint and iris) to an agent banker or ATM device and so gain access to banking services (stakeholder interviews, 2017/2018).

Reducing fraud in the health insurance sector. The health insurance sector is subject to fraud in a multitude of ways. Individuals can commit fraud by using another person's identity and health insurance information to obtain services or buy drugs for which they do not have prescriptions. Healthcare providers can commit fraud by billing for services never rendered, performing non-required services and overcharging above an agreed rate for services. The US healthcare system lost between USD70 billion and USD234 billion because of fraud in 2008 (The National Health Care Anti-Fraud Association, 2010). Healthcare providers are able to verify the identity of people who are attempting to access medications or services by analysing their biometric information. If the claimed identity of the individual does not match the biometrics information provided, the individual is denied access to services. This makes it extremely difficult for consumers to access medicine by using fake or alternative identities, as their biometrics information won't match the alternative identity. Insurers can also prevent healthcare providers from submitting false claims by requiring biometric "proof of identity" of the person who is making a claim. Healthcare providers would therefore require the person to authenticate the claim.

Falsification of identity to obtain health-related benefits and services through another person's insurance scheme has been, and continues to be, a major issue in various countries in Africa, especially in Kenya and Uganda (stakeholder interviews, 2017/2018). In response to these issues, the health insurance industry in Kenya began implementing biometric solutions that could verify the identity of patients who are seeking treatment, thereby preventing people from using fraudulent identities to gain services. The implementation of biometrics in the health insurance sector in Kenya benefits not only the individual firms but the insurance sector as a whole, which is able to operate with more confidence and certainty, possibly leading to additional, broader economic growth. Additionally, the burden on governments to deal with drug-abuse patients is likely to decrease as fraudulent access to drugs is curtailed, thus opening up opportunities to fund other developmental objectives. Given that opioid drug abuse cost the United States USD504 billion in 2015 (Gibson & Mutikani, 2017), reducing drug dependence can have a large savings impact.

Maximising the impact and reach of G2P payments. Social spending programmes (including unemployment grants, disability grants and other social spends) gain major benefits from the use of biometrics. Governments can use biometrics to ensure that their social grants are received by the intended target. This is due to the difficulty associated with falsifying an identity on a biometric system, as discussed in previous use cases. With more traditional, often paper-based systems, it is easier to use another person's documents, assume their identity and receive the social grant despite not actually being that person. This means that money that was intended for positive social and economic upliftment may not achieve such outcomes, as the recipient might spend the money less productively than the intended target, for a purpose other than the intention of the grant. Even within households, the impact of social grants can vary depending on the recipient. Van der Berg *et al.* (2015) show that in South Africa, women allocate the expenditure on a grant in a more equitable and efficient manner than men, contributing to greater health outcomes of the household. This showcases that the impact of social grants can be highly dependent on who actually receives the grant. It is therefore critical to ensure that the grants be received by the intended recipient. Biometrics can provide certainty of identity and reduce the cases in which the wrong person receives a social grant.

Increasing the efficiency and savings of G2P payments. It is also possible to receive a social grant or payment intended for a person who does not exist, has been deceased for some time or no longer works at an organisation, but is on the database as a social grant recipient. These are known as "ghost recipients". This causes massive inefficiencies in G2P systems. Money that the government could spend productively elsewhere is funnelled into the pockets of unintended recipients. By requiring biometrics authentication upon receipt of payments, it is very difficult for an individual to claim the identity of a deceased person, or a person who does not exist. Moreover, when transitioning to biometrics-based identification systems in payrolls, a biometrics audit can be undertaken to remove any identities from the database that are duplicates[11]. Biometrics therefore create savings to government by removing payments to ghost workers. In South Africa in 2012, the South African Social Security Agency (SASSA) introduced biometric cards for their social grants programme. SASSA estimated that, between 2012 and 2013, R150 million was saved as a result of the implementation (Brand South Africa, 2013). Similarly, the Aadhaar biometric identity in India saved the government millions of dollars by removing ghost subsidy recipients on its LPG subsidy database (stakeholder interviews, 2017/18). Furthermore, the use of a biometrics audit reduced the number of federal pensioners in Nigeria by 40%, creating large monetary savings[12] (Gelb & Decker, 2011).

Promoting the integrity and transparency of voter registrations. The use of biometrics in political voting processes is one of the most compelling use cases. According to Evrensel (2010), the voter registration process has a significant impact on the integrity of an election. Given the importance of fair elections in a functioning democracy, it is vital that the voter registration processes be smooth and transparent and that they have integrity. Biometrics provide a unique identity to voters (one that is difficult to fake or duplicate) and can therefore ensure the valid identity of individuals when registering.
By keeping a profile of biometrically authenticated identities on a database, it is difficult for individuals to vote or register more than once under different presumed identities, as their biometric will always link to the original identity that is captured on the database. As discussed above, biometrics also negate the need for consumers to have documents and other requirements that are often unavailable. In SSA, births are often not registered, many people don't have official identification documents and large proportions of the population are rural

[11] De-duplication refers to the process of removing duplicate identities on an identity database. During a de-dupe, the system will scan the biometrics data of a citizen against the database to see whether any other identities have the same biometrics. If other citizens have the same biometrics, this indicates that the citizen has created fake identities – because the biometrics data all link to one person. In cases where very large populations exist (such as in India), there are instances where different people have very similar biometrics. In these cases, multi-modal biometrics may be necessary to ensure that each biometric identity is unique. India uses fingerprints, face and iris biometrics features.

[12] The overall success and reach of the Nigerian National Identity Scheme are debatable, but they clearly show the impact of biometrics for specific uses cases, such as the insurance sector.

(Genkey, 2016). This makes it difficult to maintain an accurate voter's database, as individuals may lack the necessary documents to prove their identity. By using biometrics as a form of identity verification, the need for these documents is averted. Other political and civil processes, such as property licences and trading licences, also benefit from the use of biometrics, which can provide much greater certainty of the identity of traders, thus facilitating transparent transactions.

In Tanzania, the National Electoral Commission introduced biometrics into its most recent election process in response to many falsification issues that had previously arisen. The previous system purportedly did not have a sufficiently robust mechanism for detecting duplicate registrations and therefore made it possible for individuals to register multiple times. It was also unable to register changes in address and was limited in the extent to which it could detect fraudulent information. This firstly had the effect of denying some genuine voters their right to vote if they had changed address or failed to produce the correct documents on voting day (which was a direct contradiction of the Tanzanian constitution), while in other cases allowing one person to vote multiple times, ultimately skewing the results with the possibility of damaging the integrity and accuracy of the election process (Mwighusa, 2013).

The integrity of the entire election process still paramount. Cenfri stakeholder interviews (2017/2018) confirm that voting registers are one of the most essential and common use cases for biometrics in African countries. Countries such as Ghana, Kenya, Nigeria, Tanzania and Zambia have all used biometrics in their voting registers. Despite the clear benefits of using biometrics in the voting process, it should not be perceived as a panacea to the lack of confidence in voting registrations, as the reputation of the institution or entity that conducts the process still plays a major role in instilling confidence in the entire process (Evrensel, 2010). As such, biometrics can be used and are being used across the world as tools for increasing the transparency and integrity of voting procedures, but cannot alone solve issues related to fraud and transparency.

Improving civil processes. In addition to political processes, civil processes (such as property licences, trading licences, driving licences and other types of operating licences) also benefit from the use of biometrics. Biometrics can reduce fraud and increase certainty of the identification claims. Improved identification procedures within this environment can stimulate business growth and economic activity.

Reducing tax fraud. A functional, well-managed identity system is important for tax authorities, as it provides a reliable platform from which to gather tax effectively. The use of biometrics in the identity systems enhances its credibility and reliability by providing unique identifiers attached to each identity. This gives tax authorities greater confidence that they are dealing with the correct person. It also hinders the ability of fraudsters to conceal the true nature of their income. A common means of committing tax evasion is to register different licences under multiple different identities, thus splitting overall income and keeping tax within brackets that do not reflect total income. By linking biometrics to identities, fraudsters will not be able to maintain multiple different taxable identities, as they will all match with the same biometrics. Using biometrics, authorities can also ensure that tax returns are filed by the correct person. This would stop identity theft whereby individuals steal the identity of a person who is owed returns on tax for the financial year and claim that money for themselves.

Establishing an identity for asylum seekers and crisis relief beneficiaries. Biometrics provide refugees, crisis victims and asylum seekers a legitimate, usable identity that they otherwise may not have been able to establish, due to the lack of foundational documents (Farraj, 2011). The biometrics ID allows them to access critical services and to maintain an identification amidst turbulent circumstances. For example, in 2010 the Pakistan government used its national identity system (NADRA) to deliver financial aid to persons affected by severe floods that were occurring at the time. The portion of the population that needed assistance were easily identified with their fingerprints, which were linked to the NADRA database and certified their area of residence. This was particularly useful as most of them had lost other forms of paper-based ID during the floods (Gelb and Decker, 2011). As weather-related disasters such as drought become a more severe challenge across SSA, biometrics can play a vital role in facilitating the effective distribution of relief.

Improving the effectiveness of national security systems. Interviews with stakeholders (2017/2018) revealed that public security is a common use case for biometrics across Africa. Biometrics can be used to confirm the identity of people for court appearances, for criminal history checks, for criminal investigations and for tracking of criminals. For example, the biometrics found at a crime scene (such as fingerprints) can be linked to an individual and used in the investigation process. Police authorities also make use of facial recognition to track or detect wanted individuals among a crowd, through the use of public security cameras in roadways and airports. In addition, the digitisation and automation of business processes into the police management system (which includes the use of biometrics) is a strong use case in Africa, as the management of paper documents and filing often results in loss of data, damage to data and unauthorised access to data (Lyoko et al., 2016). Automation of these paper-based systems, including the addition of biometrics, have been found to increase efficiencies in police information management systems in Uganda and Zambia (Lyoko et al., 2016). Stakeholder interviews (2017) confirm this to be a major driver of the use of biometrics in Africa.

A more reliable means of access control. Biometrics are commonly used for physical access control in both the public sector and the private sector. This can be applied in a multitude of ways. For example, border control may use biometrics to verify the identity of individuals who are looking to enter a country. Border control can better regulate the movement of people between countries, as it provides greater certainty of the identity of individuals. Biometrics can also be used for access control in the education system. Some countries in Africa use biometrics in their examination sessions to ensure that the correct person takes the test. This solves the problem of professional "test takers" faking their identity and receiving payments for taking the test on behalf of the actual student (Credence ID, 2017).

Barriers

The use cases discussed above give an indication of the outcomes that can be achieved through the effective uptake of biometric identity programmes within the financial services sector and broader society. However, efforts to implement such systems are not always successful due to a multitude of potential barriers that can arise or may be present. Regulators, FSPs and donors will need to be cognisant of these barriers when they consider implementing biometric systems in Africa.

Lack of harmonisation between biometric systems within African countries. Stakeholder interviews (2017/2018) revealed that many biometric initiatives exist in Africa. However, they tend to exist as silo initiatives that are built for specific industries, such as the national security, the banking industry, or the voter's registries. The many systems that might exist within one country are often built from scratch, requiring massive resources, rather than building on and using the systems created by other biometrics initiatives. This leads to inefficiencies, over-spending and multiple digital identity systems in one country. These "silo systems" are developed differently and comply with different biometric standards, which means that they cannot interoperate with one another. Biometrics need to comply with the same standards for the devices and technology to interoperate. This means that individuals need a unique biometrically linked identity for each use case, as opposed to verifying their identity with one biometrically linked identity. In Ghana, for example, there are separate biometric systems for the national ID, vehicle licensing department, National Insurance Trust, passport office, voter registration system, and law enforcement. Each of these systems underwent a separate enrolment process and uses different biometric devices and standards (stakeholder interviews, 2017/2018). Consumers therefore have multiple different biometric identities that can be used for specific use cases. It is more efficient to have one robust digital identity that institutions can link to when verifying identities, rather than each institution creating its own biometric database and digital identification system.

Competition between governmental departments making harmonisation difficult. Intergovernmental relations are competitive, unaligned and uncoordinated. This leads to inefficiencies in service delivery and output and has contributed to haphazard development of biometric identity initiatives (stakeholder interviews, 2017/2018). It acts as a key barrier to harmonisation. The competition and conflict between departments make it almost impossible to harmonise biometrics approaches. For example, in Nigeria the National Registration Institution (NRI) is mandated to consolidate the separate biometric databases across the country but is encountering significant resistance from other departments in implementing this. In Ghana, the National Identification Authority (NIA) is mandated to be the identity management body in the country, yet separate governmental departments have developed their own biometric identity systems and do not coordinate with the NIA (stakeholder interviews, 2017/2018). This conflict is damaging for development, and it hampers opportunities for integration. Moreover, in some African countries, mandates prevent governmental departments from interlinking and working together. This all creates an ecosystem of mandate-driven developments, which fail to take the bigger picture into account, focusing on short-term solutions to immediate problems.

Uncoordinated donor funding resulting in incongruent systems. Compounding the issue discussed above is the lack of coordination among donors regarding the funding of biometrics projects in Africa. Stakeholder interviews (2017/2018) reveal that in many African countries, governmental departments are receiving funding from donors to create new biometric systems when there are often ongoing biometric systems being implemented or already up and running within the same country. It is more cost-efficient to fund departments to link into already-existing biometrics initiatives, or to provide ICT infrastructure that would facilitate the use of biometrics across all sectors, rather than funding separate projects that end up working only within their sectors. Moreover, these systems might eventually need to be interlinked at a later stage, which would incur further costs to the donor country concerned. Therefore, it is of vital importance that donors communicate effectively and ensure that spending on biometric initiatives is done in a manner that promotes interconnectedness and takes cognisance of the *current* and *ongoing* developments.

Cost: a significant barrier without multiple use cases. National biometrics systems are expensive to implement and require the participation of both public-sector and private-sector players to maximise their usefulness. Lack of funding was identified as one of the reasons for the failure of biometric implementations in many countries in Africa (stakeholder interviews, 2017/2018). The initial capital cost depends on the type of biometric solutions being implemented, the number of different biometrics being assessed and the infrastructure available to facilitate the process. A robust and reliable biometric identity would likely require at least two different types of biometrics and would therefore require a large initial capital expenditure to implement. Despite large capital costs, the use cases described above create savings opportunities to recoup and eventually create greater savings than the initial cost, but they would need to be incorporated into the initiative from the outset. Use cases also depend on the behaviour of the consumers and industries alike. If a biometric identification system is initiated, but private-sector players or consumers do not make use of it, then it will not recoup the savings. It is therefore important that a coordinated and transparent approach be taken when funding these initiatives. The success of the Nigerian Bank Verification Number (BVN) was predicated on the cost-sharing arrangement between the central bank and the private sector. The Central Bank paid half of the initial capital costs, while private banks (which are part of the bankers committee) paid the other half (stakeholder interviews, 2017/2018). Each bank pays based on its relative market share, resulting in a successful implementation process.

The nature of work in Africa degrading biometric characteristics. In many developing countries, the majority of the workforce is engaged in physical labour as a source of employment. This is no different in Africa, where many workers engage in mining activities, construction and other physical labour. This kind of work often affects the readability and clarity of biometric characteristics, especially fingerprints, because the skin on the hands and fingers gets damaged, smoothened or distorted. This can cause fingerprints to be degraded to the point where they cannot by read by biometric devices, as there are not enough distinguishable minutiae points that can be used to generate high-quality templates. This results in workers being unable to enrol in biometric identity programmes, because the biometric devices cannot capture high-quality images to meet standards or assert an identity with confidence. This problem is widespread across Africa and is not specific to any jurisdiction or country (stakeholder interviews, 2017/2018). It is therefore important to assess the size of the population and the nature of work within the country. Fingerprints cannot be the only form of biometrics implemented in African countries with large populations and/or large portions of the population engaged in physical types of work. A similar model to the Aadhaar model (where fingerprints *and* iris scans are used) would be more applicable to countries with large populations employed in physical labour, but this implies increases in capital costs.

Infrastructure constraints impeding the successful implementation of biometric systems in SSA. ICT infrastructure is critical to the efficacy of biometrics. During the identification process, the biometric information of consumers is sent to a database for storage and creation of an identity. Similarly, during verification the biometric data is compared against a stored template on a database. The process of communicating with the database where templates are stored requires an online network system with adequate bandwidth speed, as large amounts of data need to be sent to remote locations in real time. If there is no network coverage in the area where identification is taking place, it is not possible to verify the biometric identity of the individual, because the biometrics devices cannot communicate with the server. Similarly, if the network is too slow, it will take very long to verify an identity. This can be problematic if many people need to be verified in a short space of time. Stakeholder interviews (2017/2018) indicate that lack of adequate ICT infrastructure is a key impediment to digital identities and biometrics identities in SSA. Road and transport infrastructure is also important for the success of a biometric identification scheme. If certain sections of the population cannot be reached due to a lack of transport infrastructure, it is not possible to take biometrics readings and enrol them on the system.

Insufficient local capacity and training to use and maintain biometric technology effectively. Stakeholder interviews (2017/2018) indicate that the lack of skills among employees makes implementation of biometrics programmes difficult and more susceptible to failure. The methodology for capturing biometrics is usually done according to an international standard. If staff do not collect the biometrics data according to this standard, the templates might not be usable, necessitating a re-enrolment process. In addition, staff may not be trained adequately to use the biometrics software for verification once rollouts have been completed, or they may not wish to use technology that they are unfamiliar with. For example, Lyoko *et al.* (2016) argue that a key challenge in implementing automated biometric systems in police information management in Zambia is due to human resource resistance to changing or adopting new technologies. Maintaining a database of sensitive information requires highly skilled, technical staff. In some cases, biometrics service providers leave local staff insufficiently trained to deal with maintenance issues themselves, thus requiring the assistance of the service provider again (stakeholder interviews, 2017/2018). This affects the feasibility of the initiative, as maintenance costs become prohibitively high. It also affects the stability of the system, as downtimes increase and reliability decreases. This shows the need for sufficient staff training and capacity in the use of new technologies. However, the burden should not only be on the local population to familiarise themselves with the technology, but also on the biometric vendors to ensure that staff be capacitated to operate the system themselves.

Security breaches of biometrics databases having severe impacts, including the invasion of privacy. The consequences of breaches in security and identity theft are exacerbated where biometrics are involved. Despite increasing the resistance of a digital identity to fraud, if biometrics are compromised, the ramifications are more pronounced due to the nature of biometric information and the fact that it forms part of a person's physical identity. Access to such information by unauthorised persons can be considered an invasion of privacy, which is a serious concern given that privacy is a fundamental right across many cultures (Irish Council for Bioethics, 2009). This is due to the "unique" nature in which biometrics identify people and the fact that bodily characteristics are linked to the concept of the self (Irish Council for Bioethics, 2009). Therefore, invasion of biometrics data implies a serious invasion of privacy. If a person manages to gain access to the biometrics of another person, by creating a fake fingerprint for example, they could use that fingerprint across many accounts for impersonation purposes[13] (Prabhakar, Pankati, & Jain, 2003). Moreover, by hacking databases with biometric information, the digital identity of individuals could be altered. This is done by replacing original biometric templates with new ones, which may not match the owner's actual biometrics. This disables that person's ability to use their biometrics as a form of identity verification, as their biometrics would no longer match the biometric information attached to their digital identity. Finally, typical identification measures (such as passwords, PINs and signatures) may not apply to all of a user's accounts, and they can be changed if the need arises; but biometrics data is very difficult to change, with some (such as IRIS technology) being impossible to change. For example, if a person's bank account password is hacked, they can simply change the password, thus removing the compromised password. However, if their biometric is hacked they cannot change their biometric. This means that the stolen biometric data is indefinitely compromised. Even though hacked biometrics data has significant impacts, it should be noted that it is still easier to hack passwords than biometrics. As such, biometrics offer *enhanced* privacy benefits to the consumer because they provide a rapid form of identification with lower likelihood of theft, but the privacy concerns that do arise need to be noted.

Lack of public trust a potential pitfall.
In light of the privacy concerns mentioned above, citizens may be hesitant to provide, or condone the use of, their biometric data. Resistance to biometric identification varies depending on the region and country. According to stakeholder interviews (2017/2018) developed-country citizens tend to offer more resistance to authorities capturing their biometrics than citizens from developing countries. However, this does not mean that cultural or societal positions on the use of biometric data are necessarily positive in developing countries. The stakeholder interviews (2017/2018) also revealed that citizens are generally hesitant to give their biometric details to governments, for fear that the data will be used to tax them more or to monitor their movement. The lack of willingness to participate in biometric programmes due to a lack of trust in authorities can reduce the effectiveness of the rollouts and the sustainability of the system. Citizens may initially refuse to allow the capturing of their data or may protest at the use of their data if breaches in security are suffered or if their data is used for purposes other than the original intent. It is therefore important to ensure that a fundamental trust relationship be established between the

[13] This has become much more difficult to do with recent advancements in fingerprint scanners.

organisation that captures the biometrics and the citizens of the country. It is also vital that the integrity of the database be sustained and that the damages suffered from security breaches be minimised so that confidence and trust in the organisation and system be maintained.

Regulation

Establishing a biometric-based identity system (as part of a national, financial or other identity system) requires a well-developed and encompassing legal and regulatory framework to support it. Given the sensitive nature of biometrics and other key identity data, the need to protect, manage and control the use of this data becomes extremely important. This sub-section provides an overview of the areas that need to be covered in the legal and regulatory frameworks to support digital identities, which include biometrics.

The state of legal and regulatory frameworks for identity in Africa.

According to The World Bank (2017), the majority of African countries currently lack the legal and regulatory framework to support modern identity systems. Cenfri stakeholder interviews (2017) confirm that most countries have implemented biometric identities without first implementing the necessary regulatory frameworks. Only two countries in Africa (Côte d'Ivoire and Morocco) are identified by the World Bank (2017) as having adequate legal and regulatory frameworks for modern identities. In most cases, countries have no laws in place for the ownership and use of personal digital data, have many overlapping mandates or have unclear jurisdiction over registration and identification processes.

Embedding the principles of privacy by design. A country looking to facilitate the successful development of biometric identity systems should seek to create a regulatory ecosystem that embodies the principles of *privacy by design* as depicted by Cavoukian (2009) and incorporated in the EU General Data Protection Regulations (GDPR). This will initially require the implementation of effective policy that clearly defines the vision of the digital identification system and the intention to embed privacy into the design. These key principles are depicted in the table below.

Principle	Description
Proactive, not Reactive; Preventative not Remedial	Focus on preventing privacy invasion events rather than reacting to them
Privacy as the Default	No action should be required by the individual to protect their data, IT system should protect them by default
Privacy Embedded into Design	IT systems are built with privacy in the design. Privacy features are not added afterwards.
Full Functionality – Positive-Sum, not Zero-Sum	No trade-offs are made. Privacy by design should facilitate privacy *and* security, and should not make any trade-offs for the sake of privacy.
End-to-End Security – Lifecycle Protection	Data should be securely retained during lifecycle and destroyed effectively at the end of the lifecycle.
Visibility and Transparency	Visibility and transparency that business practices related to the use of the private data are following stated promises and objectives, subject to independent review.
Respect for User Privacy	Keeping the interests of the individual as top priority

Table 1: Principles of Privacy by design

Source: Cavoukian (2009)

Key legal and regulatory areas. In light of the above, the key legislative areas that need to be covered to ensure a successful digital identity or biometric identity programme are summarised in Figure 5 below. It is important to cover all areas adequately as any issue arising in each of these areas could cause the system to derail.

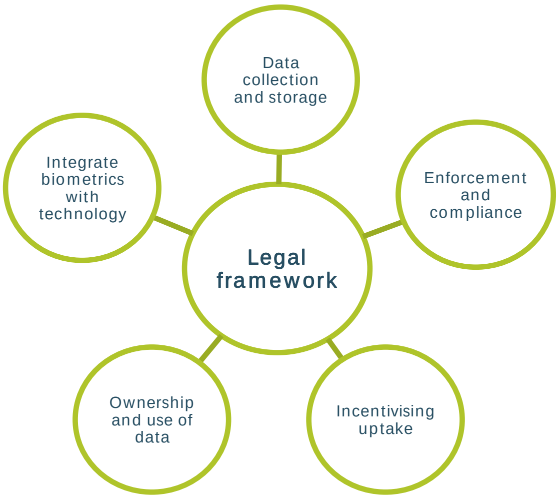
Data collection and storage
Integrate biometrics with technology
Enforcement and compliance
Legal framework
Ownership and use of data
Incentivising uptake

Figure 5: Legal and regulatory framework

Source: Authors' own

Need for laws regarding the storage of data. To sustain a digital identity database, it is important that the storage of personal identification data (including biometric data) be legalised in the country, as some African countries are yet to legalise the storage of biometrics data (stakeholder interviews, 2017/2018). If biometrics or identity data cannot be stored, it is not possible to perform identity and verification checks against databases, which would defeat the point of the initiative. To ensure privacy, the data should be stored in template form (which is a digital representation of a biometrics image) rather than representing an actual image. Stored data should be encrypted to make the data as secure as possible.

Controlling access to and use of biometric data. It is important to clearly define the boundaries regarding usage of, and access to, sensitive identity and biometric data. Firstly, citizens should own their identity data and be in a position to give consent to the use of their data, should they deem it appropriate. This is in line with the International Bar Association's (2016) recommendation that "it is more appropriate to ascribe ownership of personal information to the persons to whom that information relates". If consent to use the person's data is granted, only the necessary parts of the data should become available, and only for a specified period, after which the data goes back into encrypted storage. For example, a bank that wants to enrol a potential client should only be able to access biometric data that it requires for verification purposes and not all the data that may relate to the client's digital identity. The laws should clearly state that the data can only be used for the intended purpose.

Penalising infringements. The legal system needs to make clear the consequences of infringements related to either the misuse of data for some purpose other than the intended use, the theft of data, and/or the loss of data. This could have happened intentionally or as a result of negligence. In France, the National Data Protection Authority is responsible for oversight of data storage and use. They perform inspections and issue compliance orders if companies break the law. French criminal code dictates that misdemeanours are punishable for up to five years in prison (World Bank, 2015). The EU GDPR (2016) states that organisations in breach of the GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater). Breaches can typically include: not having sufficient customer consent to process data, violating the core of Privacy by Design, not notifying the supervising authority and data subject about a breach, or not conducting an impact assessment. Regulatory authority should make clear the penalties for breaching laws related to the privacy of data, particularly sensitive biometric data.

Incentivising uptake. Broader societal benefits like governance can only accrue with substantial uptake of the identity of the system. If biometric identity systems are not fully supported by the public, or the public is agnostic to the use of the biometric identity system, it is important to incentivise uptake through regulations. This is generally done by withholding access to advantageous government services unless the citizen has enrolled, or by enforcing enrolment. For example, in Aadhaar, citizens were unable to access the cooking gas subsidy without proving their identity through their unique Aadhaar number (stakeholder interviews, 2017/2018). In Nigeria, The Central Bank of Nigeria took a more direct approach in regulating the uptake of the BVN project, by implementing a series of requirements for banks. For example, Central Bank of Nigeria (2014) explicitly fast-tracked the BVN process by requiring all deposit money banks (DBMs) to enrol at least 40% of their customers with BVN before 31 December 2014 and to fully integrate their core banking system with BVN by 3 November 2014. It also stated that all credit customers had to have BVNs by 31 December 2014. The decision on whether to enforce or incentivise participation will depend on each individual country and the expected outcomes.

Recognise digital as a foundational proof of identity. To maximise the usefulness of biometric identities for the economy and especially the financial sector, digital identities and biometrics need to be integrated into society in such a way that they are legally recognised. Firstly, electronic ID (eID) biometrics should be explicitly recognised as a population record and a valid, foundational identity record. This ensures that digital identity can be used as the primary tool for identification purposes. Furthermore, biometrics itself should be recognised as a valid population record and foundational identity. This allows biometrics themselves to legally verify the identity of individuals. Thirdly, the use of electronic signatures or biometrics in payments, contracts and communication processes should be legalised. This allows people to authorise transactions by using an electronic form of signature, such as a biometric.

Integrate with the financial sector. To really see biometrics enhance access to finance and reduce compliance cost for banks, biometrics need to be legally recognised as a valid form of identity for the CDD process in financial services. As discussed in the use cases section, the potential for biometrics to improve access to financial services by removing the need for paper-based identification documents, as well as PoA, is immense. However, without the necessary regulation to accompany the technology, it cannot be implemented properly. For example, in Kenya, banks are able to verify the identity of their customers by comparing a provided biometric against the National Identity database. This is used for the CDD procedure to enhance certainty of the identity of potential clients (stakeholder interviews, 2017/2018). However, AML regulation still requires that other identity documentation such as proof of address and ID be present as part of the CDD process. As such, despite biometric technology being in place, its usefulness is withheld by the lack of accompanying regulation.

Standards and interoperability

Utilisation of international standards necessary to ensure interoperability between biometric systems. The use of templates in biometric identities is necessitated by the need to ensure privacy. Reviewing raw data images would entail an analysis of the actual biometrics of a person, whereas a template is a numerical representation of the biometric images. It is therefore important that biometric templates be utilised for analysis purposes. However, the use of templates over images creates interoperability issues. More specifically, templates created under different initiatives are often created according to different standards and therefore cannot interoperate. That is, a biometric template created under an initiative undertaken in the insurance industry may not be usable as an identity for voter's registration, because the template does not meet, or differs from, standards applied for the voter's identity. Consequently, separate biometric identities are required per industry when biometric standards are not applied consistently. This problem can be avoided by ensuring that the various biometric initiatives make use of the same standards and avoid the use of locked-in proprietary vendor standards. International standards on biometrics and digital identification exist, which should be consulted and utilised to ensure interoperability. Standards for each type of biometric are published by the International Organisation for Standardization (ISO).

Harmonisation of biometric systems feasible. It is possible to harmonise biometric databases and systems that have been separately developed according to different processes and different standards. While it is not the desirable methodology to adopt from the outset, it is still possible and feasible to connect these disparate systems. According to stakeholder interviews (2017/2018) this can be done with access to the system source code, which in turn can enable access to initial biometric files. With access to the original files, the data can be converted into a standardised template that is readable across other systems. If some of the original data is of poor quality, methodologies exist that can be applied at differing levels of verification and re-sampling to bridge the quality gap cost-effectively and with appropriate risk over time, ultimately ensuring that all the templates meet the same standard while materially shortening the new enrolment cost and time to scale. However, service providers are generally reluctant to provide source code and source information to clients, as this eliminates effective lock-in to the vendor, allowing other vendors to compete. This is understandable given the competitive environment and the high costs and risks associated with installing biometrics infrastructure in a country. If service providers are not given certainty on maintenance operations across a few years, profitability is decreased. However, the importance of linking disparate biometric systems cannot be understated, as it is beneficial for the broader development of the continent and creates strong linkages between countries and between departments in governments, thus greatly affecting the ability of citizens to attain key services.

5 A roadmap for the implementation of biometrics

This note has thus far positioned biometrics as a key component of robust identity systems and a potential facilitator of financial inclusion. Building on the use-cases and barriers discussed, this section provides a roadmap for institutions that are looking to implement or incorporate biometric identity systems in their country or industry. It should serve as a key consultation piece that provides guidance regarding the various areas that need to be addressed. The following figure provides a high-level illustration of the areas that need to be addressed at each stage of the process. Following this, each area is discussed in more detail.

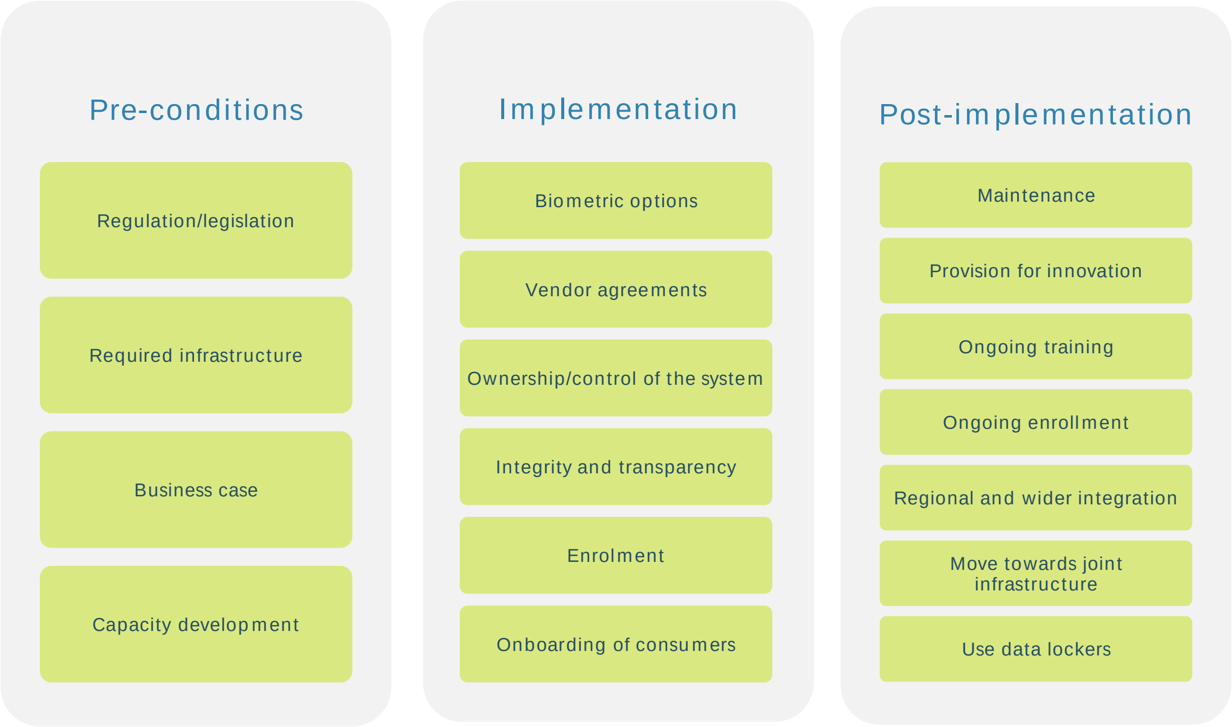

Figure 6: Summary of biometric roadmap

Source: Authors' own

Pre-conditions

Pre-conditions refer to the necessary things that need to be in place prior to implementing a biometric identity system. These vary in level of importance, with some being critical and others less critical but beneficial to the process. Institutions need to first ensure that critical pre-conditions be in place before rolling out the implementation phase of biometric projects.

Regulation. The regulatory environment plays a vital role in the successful operation of business environments, and this is no different in the case of biometrics and identities. Regulation is critical for defining roles and responsibilities within the environment (ensuring that the rights of citizens are protected), guidance to business on how to implement processes within the legal boundaries, and penalties for infringements. The following legislation needs to be in place before implementing a biometric system:

- **Electronic Communications and Transactions Act**

  An Electronic Communications and Transactions Act generally provides for the facilitation and regulation of the use of electronics for the purpose of communications and payments. In addition to providing the framework from which electronics can be embedded into communications and transactions within an economy, this Act should specifically recognise electronic identity (eID) as a valid *foundational* identity. By accepting eID as a foundational identity tied to an individual, the need for paper-based documents for POA is removed, allowing institutions to verify individuals through electronic means. It should also stipulate that electronic signatures are an acceptable form of signature and particularly that a validated biometric can be an acceptable form of biometric signature.

- **Financial Intelligence Act**

  The purpose of a Financial Intelligence Act is to prevent crime within the financial sector, which is generally in the form of money laundering and the financing of terrorist and related activities. By gathering information about the financial sector and the affairs of financial entities of interest, it is possible to control or counter financial crimes. Firstly, this Act needs to be put in place (if not already in place), but it also must explicitly assert that e-KYC[14] is an accepted form of KYC at financial

[14] KYC refers to the Know-Your-Customer process, otherwise referred to as CDD.

institutions. That is, that electronic identities are acceptable as forms of KYC during the onboarding process. Regulation should also incentivise or mandate the use of e-KYC by banks and financial institutions to ensure that overly risk-averse behaviour is not adopted, whereby financial institutions choose not to accept e-KYC despite it being stipulated in regulation that it is an acceptable form of KYC.

- **Citizens Act**

  The Citizens Act provides guidance for all matters related to citizenship in a country, including the acquisition, loss or resumption of citizenship. The Citizenship Act should explicitly recognise biometrics as a population record and a valid foundational identity. This enables citizens to use their biometrics as proof of identity.

- **Privacy Law**

  Privacy law deals with the regulation of data and information pertaining to the personal identification of individuals. This may govern who can or cannot access a citizen's personal identifiers, how the data is stored and who owns it. This law is particularly vital for biometrics due to the sensitive nature of biometric data and the need to protect citizens' biometric data. Leaks in privacy will degrade trust in the system, which is vital to the ongoing support and use of biometric systems. The privacy law should make clear who owns the data, who controls the data, who is able to access the data and for what periods, as well as penalties for data leaks that were intentional or as a result of negligence. Having this privacy law in place prior to implementation gives sight of the boundaries within which the biometrics programme must exist to ensure that privacy is fully protected in line with the law. This law should also give clarity as to the storage and/or processing of personal identification data internationally to enable possible multinational scale while still maintaining privacy.

- **Biometrics Act**

  In addition to the above essential Acts, a biometrics Act is a possible addition that could provide for the harmonisation of various legislature and acts or give certain legislation preference over other legislation where there is ambiguity. This Act would also indicate the recognised international standards for biometrics and provide for harmonisation of standards to ensure interoperability. If no biometrics Act is in place, the above standards should feature in the Electronic Communications and Transfers Act.

Required infrastructure. It is important to ensure that the necessary infrastructure be in place prior to implementation. Infrastructure should be able to facilitate the successful identification, verification and ongoing use of electronic identities to secure services or prove identity for some other means. Without necessary infrastructure, the ecosystem will collapse, as the use cases cannot be effectively tapped into.

- **Adequate ICT infrastructure and networks**

  Identification and verification of individuals will require communication with servers where databases are stored. Without adequate network coverage, users may not be able to connect to databases. Based on the current level of network infrastructure, a decision will need to be taken on whether to use regional or offline databases for when coverage is low due to unavailability of network or temporary network downtimes. Speed is also important, as slow networks cannot process multiple requests at a time in an acceptable timeframe. The size of the population and expected frequency of requests will determine the required speed, necessitating offline databases or network upgrades. Secured offline databases, which can be regional or institutional subsets of the main dataset, can be held by institutions that use the biometrics and can be used when network issues are prevalent.

  The location of the database is also important and has implications on cost. A decision will need to be taken on whether to host the database locally or internationally. This will have impacts on the cost and ICT structure, and the decision will depend on the relative security and cost associated with each option and the regulatory framework as discussed above. There should always be at least one redundant backup to the host server so that issues with the host server do not adversely interrupt service delivery. The security of the database and its resilience to hacks/leaks should be prioritised.

- **Assessing the state of the population register**

  Before implementation, the current state of the population register should be assessed. If it is in a good state, it can be used as a guide on who to enrol biometrically and should link citizens' profiles to their biometrics. If the state of the register is in disarray (as is the case in some African and Asian countries) or if there is no civil registry, it may be more efficient and expedient to create a new population register using the biometric enrolment. Enrolment in the biometric identity scheme (which forms part of the population register) should be incentivised to encourage the population not to opt out of the system.

- **Road and transport infrastructure**

  It is also important to have adequate road and transport infrastructure. Otherwise the enrolment phase is difficult to undertake.

If much of the population resides in rural areas with sparse or degraded roads, it is more difficult to reach them and to take biometric readings. The implementation phase should consider making use of the most accessible locations as enrolment points to gain early scale and then move to the less accessible and less concentrated points over time.

Business case. The viability of biometric identity initiatives depends on its usefulness within the society/economy. The more use cases that can be tied to the biometrics, the more viable it becomes – especially when compared against the relative cost of implementation. If one biometric identity system can be utilised by the health insurance sector, national security, the financial services sector, and border control, it is likely to more than recover its capital and operational costs. It is therefore important to assess the use cases for the identity system and to ensure that there is adequate demand.

- **Which biometrics to use?**

  Depending on the use cases, size of population and level of certainty required, different combinations of biometric authenticators are appropriate. In Africa the nature of work often involves physical labour, which tends to degrade biometrics – especially fingerprints, which become worn down, making it difficult for biometric devices to extract templates from them (stakeholder interviews, 2017). This may necessitate the use of additional biometrics, such as iris. For large populations, one biometric template may link to many possible candidates, as is the case in India, where the population is over a billion. This requires additional biometrics for more granular verification. One consideration is the possible need for regional or ultimately continent-wide biometrics to enable trade and hence to design local system standards with a higher scale in mind.

- **Interoperability and integration**

  Interoperability should be part of the design of biometric systems. Business and use cases are maximised if the biometrics can link to various industries. It is therefore important to ensure compatibility with other already-established biometric solutions or to create a system that can easily be connected to. The system should ideally be aligned for integration into regional systems and standards in line with political incentives, as well as regional and continental commitments.

- **Economic feasibility**

  To determine the most effective approach to implementation, a cost-benefit analysis should be conducted to determine the capital and operational costs of various approaches against their expected benefits. This would highlight, among other things, the most ideal biometrics to be used and the preferred method of enrolment. This will depend highly on what infrastructure is already in place. Scenario planning should also be undertaken to plan for different possible outcomes, which may unravel over the course of implementation. This can take into consideration regulatory and infrastructural milestones. The feasibility study should investigate:

- What use cases are there for consumers?
- How are livelihoods of consumers affected?
- What are the use cases for industries and businesses?
- Which industries will want to make use of the biometric identity? (If within the financial services sector, will banks be interested in participation?)
- How can government and corporate savings be monetised over time to finance the programme?
- How can savings and costs over time between government departments be offset to fund the programme? (Typically, the department investing in the system is different from where the tangible financial benefits accrue, e.g. Home Affairs vs Social Service Payments vs Public Administration vs Treasury.)
- What are the short-term versus long-term costs and benefits of the system?

Incentivising participation. For the initiative to be a success, the public has to buy in and participate. This can be a challenge, especially where there is resistance to technology changes or where citizens are concerned about how their data will be used. India incentivised participation by linking key social benefits to the Aadhaar identity, such as the cooking gas subsidy (stakeholder engagement, 2017/2018). Nigeria took a more direct approach by forcing all banks, through regulation, to enrol customers in BVN. Banks needed to meet certain targets within specified timeframes. Moreover, customers without BVN would not be able to access services (stakeholder engagement, 2017/2018). During implementation, incentives will need to be in place to ensure that customers have a genuine need to enrol quickly at scale. Otherwise they may opt out of the system. Existing biometric databases in the private sector could be incentivised to pre-enrol systematically, provided the requisite legal frameworks and interoperability/dataset conversion functionality is in place.

Capacity. The capacity and skill of individuals in the country are important for ongoing operation of a biometric ecosystem. To maintain and run a digital database with sensitive information as contained in biometrics requires all levels of IT skill. Databases, servers and communications networks need to be operated and maintained by technicians, while cyber-security experts would ensure that the data remains protected from attacks. Legal professionals and auditors are necessary for ensuring that the system operates within legal and regulatory boundaries. Without individuals with the capacity for fulfilling the above roles, it will be challenging to maintain the system effectively. If systems go down for extended periods and there are not enough IT professionals to fix issues, trust in the system is degraded. Before implementation of biometric systems, a plan needs to be in place to develop the capacities of local staff to resolve issues rather than an ongoing dependence on vendors.

Implementation

Harmonisation. The implementation process should keep harmonisation and integration with other systems at the forefront of its priorities. Rather than operating in silos, institutions should leverage on one another as much as possible to maximise efficiency, minimise cost, and increase convenience for the consumer. Therefore, new biometric initiatives should always draw on other previously implemented systems as much as possible so as not to duplicate work that has already been done. It is possible and feasible to harmonise biometric systems so long as the original source code from previous databases can be accessed. With access to the source code, new initiatives can access the original biometric images. These images can then be assessed for conformity with the standard being applied. Images can then be converted into the required format; or if the quality of the image is insufficient, select individuals can be re-enrolled and the outstanding information can be captured.

Enrolment process. The enrolment process will depend on the current state of affairs in the country and how many other biometric initiatives have already been implemented prior to the initiative, either through government or private sector. If there is already a comprehensive database with high-quality biometric data, it is better to simply link to that database rather than creating an entirely new one. However, in most cases this is unlikely, as biometric initiatives have been haphazard and disharmonised in Africa (stakeholder interviews, 2017/2018).

- **First enrolment.** For those users who are not currently on biometric databases throughout the country, an initial or "first enrolment" will need to take place, whereby users provide their biometric information and a new biometric identity profile is created for that person.
- **Second enrolment**. Citizens who already have biometric identity profiles with other institutions may need to re-enrol with the new initiative, depending on the quality of the current biometric images they have provided and whether those images comply with the international standards as set out in the legislation. A re-enrolment will recapture or capture the damaged/missing data to complete the user's profile. Biometric data will first have to be assessed and ranked to determine which profiles need revisions/additions, if they need such at all. Ideally re-enrolment will occur over time and in a risk-proportionate manner, i.e. where the level of risk of error is material to the transaction value at risk.
- **De-duplication**. As new people enrol, the system would need to run de-duplications to remove double entries in the system. This can either be done as people enrol or after batches of enrolments. Ideally new enrolments

should only be validated and incorporated into the dataset after successful de-duplication.

Vendor agreements. Agreements with biometric vendors need to be concluded with the long-term interest of the country and scheme in mind. Governmental departments or other institutions should ensure that access to the source code be included in the agreement so that the original images can be accessed at later stages and converted to different formats if necessary, ensuring original data could be compatible with other legacy devices or new devices that come into the market.

Integrity and transparency. Successful implementation needs buy-in from the public. Issues that may arise during the course of implementation will affect the public's perception of the project, especially if privacy issues arise. Trust in digital services, especially biometric-based, requires trust that is maintained by ongoing usefulness and stability of the system. The implementation process should therefore be transparent, and there should be public milestones that can be used to assess the implementation process by all affected parties. There needs to be a comprehensive communication strategy to keep the public aware and informed.

Upskilling and capacity enhancement. During the implementation process, it is important to maximise skill growth and retention among the local population. All teachable moments, such as the onboarding process, should be leveraged to educate consumers and promote acceptance through demonstrated consumer value.

Post-implementation

After implementation, the project should have ongoing support and maintenance to sustain usefulness and longevity. As discussed, downtimes and system failures can cause loss of trust in the system, thus stimulating the collapse of the identity initiative.

Maintenance and security. The pricing strategy for the initiative should include cost of ongoing maintenance and upgrading of the infrastructure to accommodate innovation and expansion of use cases. This also includes the ongoing costs associated with maintaining the security of the database for protection against attacks. Maintenance of records and the security of the records and database are a paramount ongoing cost.

Provision for innovation. Throughout operation, there should be adequate scope to allow improvements to the system in terms of value-added services as well as improvements in technology. This will require open-source architecture. Open-source architecture allows third parties to establish valuable services that link to the identity database, thus expanding its usefulness and scope. As technology evolves, there should be adequate space for the system to adapt to new technologies and remain current. This decreases the chances of the system becoming outdated and losing value.

Ongoing training. Ongoing training and teaching of consumers and staff should occur to ensure that the system is utilised as efficiently as possible and that it remains relevant within current technological advances.

Ongoing enrolment. Following implementation, consumers who were not enrolled in the initial and secondary enrolment phase should be enrolled over time. This can be done as customers demand access to the services that require the ID. In addition, regions within the country which are more remote and more difficult to reach may not have been covered in the initial enrolment phases. The initiative should continuously seek to enrol citizens from these areas over time, where feasible.

Regional and wider integration. As identity initiatives within the region expand, regional integration should be prioritised to ensure interoperability across regions. This allows for levels of robust risk mitigation in both sending and receiving countries regionally. This will enhance risk mitigation procedures at a regional scale and the reputation of FSPs in terms of financial integrity. This is likely to decrease de-risking and have a positive impact on financial sector development within the region.

Move to joint infrastructure and processing facilities. Countries should move towards using processing facilities/hubs at a regional level to leverage scale and make better use of limited expertise. Databases and processing can be done at regional level to reduce the regional competition for scarce capacity.

Move towards using data lockers. Data lockers keep sensitive data private and release the data on consent of the user for specified periods. Where data lockers are not already in place, countries should continuously move towards using data lockers for additional use cases such as medical data.

6 Conclusion

This note has positioned biometrics as a potential solution to the issue of identity in Africa and sub-Saharan Africa. However, implementation of biometric identity systems comes with its own unique set of challenges and hurdles to overcome. The note has outlined both the use cases as well as the challenges with biometrics. It has ultimately provided a roadmap for implementing biometrics, which guides stakeholders on how to go about implementing these identity systems while avoiding pitfalls. Key findings are summarised below.

Harnessing biometrics for the financial sector. Biometrics can be utilised in the financial sector to decrease the burden on consumers to have paper-based ID documents and proof of address. In addition, FSPs' cost of compliance with CDD procedures and compliance risk decreases significantly by using biometrics as an identification tool. However, it is important to have adequate legislation and regulation, as well as ICT infrastructure, in place to support the use of biometrics as an identifier.

Building systems with harmonisation in mind. Many of the biometric identity systems in Africa have been developed separately and are not interoperable with one another. Future systems should keep in mind that the benefit of biometric identity systems is enhanced when they are able to tap into multiple use cases. Therefore, systems should be set up according to specific designated standards, based on open-source architecture so that future developments can link into the system.

Leveraging on what is already in place. The research has found that harmonisation of previous systems is indeed possible and feasible. This negates the need to start from scratch when implementing a new biometric identity system. It allows new initiatives to leverage on legacy infrastructure to decrease the costs of new initiatives and to ensure that legacy systems remain relevant by integrating them. By accessing the source code of other identity databases, it is possible to alter templates to be interoperable on other systems. New identity systems need to assess what is already in place before initiating the system and initiating any enrolment process, and leverage on them to enhance linkages between industries, reduce costs and increase convenience for the consumer.

Privacy never to be compromised. Maintaining the integrity of databases and the privacy of sensitive personal and biometric information is integral to achieving a functional biometric identity system. Consumer trust in the system is essential for its ongoing use. Stakeholders should embed privacy into the design of the identity system.

7 References

Bankable Frontier Associates. (2018). Landscaping a digital financial identity. FinMark Trust.

Bester, H., Chamberlain, D., De Koker, L., Hougaard, C., Short, R., Smith, A., & Walker, R. (2008). *Implementing FATF Standards in Developing Countries and financial inclusion: findings and guidelines.* First Initiative.

Brand South Africa. (2013, August 22). *Biometric grant cards beating fraud.* Retrieved from Brand South Africa: https://www.brandsouthafrica.com/south-africa-fast-facts/social-facts/grants-220813

Cavoukian, A. (2009). *Privacy by Design: the 7 Foundational Principles.*

Central Bank of Nigeria. (2014). *Circular 01/015: Clarification Circular on Bank Verification Number (BVN) Enrollment.* Abuja: Central Bank of Nigeria.

Consult Hyperion. (2017). *Biometrics in Digital Financial Services.* FSD Africa.

Evrensel, A. (2010). *Voter Registration in Africa: A Comparative Analysis.* Johannesburg: EISA.

Farraj, A. (2011). Refugees and the Biometrics Future: The impact of Biometrics on Refugees and Asylum Seekers. *Columbia Human Rights Law Review*, 891-942.

Financial Action Task Force. (2012-2018). *International Standards on Combatting Money Laundering and the Financing of terrorism: The FATF Recommendations.* Paris: FATF.

Findex. (2014). World Bank.

Gelb, A., & Decker, C. (2011). *Cash at Your Fingertips: Biometric Technology for Transfers in Resource-Rich Countries.* Washington DC: Center for Global Development.

Genkey. (2016). *Delivering Biometrics Elections.* Genkey.

International Bar Association for Human Rights. (2016). *Digital identity: Principles on Collection and Use of Information.* IBAHRI.

International Financial Corporation. (2012). *Credit Reporting Knowledge Guide.* Washington DC: International Financial Corporation.

Irish Council for Bioethics. (2009). *Biometrics: Enhancing Security or Invading Privacy.* Dublin: Irish Council for Bioethics.

Iritech. (2016, December 30). *e-KYC Is Growing Significantly in India.* Retrieved from Iritech: http://www.iritech.com/blog/ekyc-1216/

Jain, A., Flynn, P., & Ross, A. (2008). *Handbook of Biometrics.* New York: Springer.

Lyoko, G., Phiri, J., & Phiri, A. (2016). Integrating Biometrics into Police Information: Management System: A Case of Zambia Police. *International Journal of Future Computer and Communication*, 1-7.

Mastercard. (2017, April 20). *Press Releases: Mastercard Unveils Next Generation Biometric Card*. Retrieved from Mastercard: https://newsroom.mastercard.com/press-releases/thumbs-up-mastercard-unveils-next-generation-biometric-card/

Mohan, R. (2006). *Economic Growth, Financial Deepening and Financial Inclusion.* Reserve Bank of India.

Mwighusa, D. (2013). Transforming Voters Registration Paradigm in Tanzania, The Shift from OMR to BVR. *International Journal of Science and Research (IJSR)*, 1064-1068.

Prabhakar, S., Pankati, S., & Jain, A. (2003). Biometric Recognition: Security and Privacy Concerns. *IEEE Security and Privacy*, 33-42.

Saini, R., & Rana, N. (2014). Comparison of Various Biometrics Methods. *International Journal of Advances in Science and Technology*, 24-30.

The European parliament. (2016). *EU General Data Protection Regulations.*

The National Health Care Anti-Fraud Association. (2010). *Combatting Health Care Fraud in a Post-Reform World: Seven Guiding Principles for Policy Makers.* New York: NHCAA.

Thom, M., Cooper, B., Weideman, J., Coetzee, W., Gray, J., Hougaard, C., & Plessers, H. (2016). *Making Access Possible: Democratic Republic of Congo.* UNCDF.

Van der Berg, S., Siebrits, K., & Lekezwa, B. (2015). *Efficiency and Equity Effects of Social Grants in South Africa.* Stellenbosch: Bureau for Economic Research.

World Bank. (2014). *The Global Findex Database.*

World Bank. (2015). *Identification for Development (ID4D) Integration Approach.* Washington DC: World Bank.

World Bank. (2017). *Identification for Development (ID4D) Global Dataset.*

World Bank. (2017). *The State of Identification Systems in Africa.* Washington DC: World Bank.

Annexure: List of stakeholder interviews

Country	Organisation	Date of meeting
Tanzania	Bank of Tanzania	7/11/2017
Malawi	Central Bank Malawi	7/11/2017
South Africa	Paycode	25/10/2017
Nigeria	Identity Commission of Nigeria	10/11/2017
Ghana	I.D4Africa	10/11/2017
Africa-wide	I.D4Africa	17/11/2017
Zambia	Central Bank of Zambia Payments Division	17/11/2017
Nigeria	Nigeria Payment System	21/11/2017
Kenya	Kenya Bankers Association	24/11/2017
International	WCC	7/12/2017
International	Idermia	8/12/2017
International	GENKEY	15/12/2017
International	OECD international	15/12/2017
International	Credence ID	18/12/2017
India	Bankable Frontier Associates (previously UIDIA)	22/02/2018

cenfri

Centre for Financial Regulation and Inclusion
Cape Town, South Africa
info@cenfri.org
@cenfri_org
www.cenfri.org

fsdafrica

FSD Africa, Nairobi, Kenya
info@cenfri.org
@FSDAfrica
www.fsdafrica.org

UKaid
from the British people

Department for International Development
inquiry@dfid.gov.uk
@DFID_UK
www.giv.uk

About Cenfri

The Centre for Financial Regulation & Inclusion (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 seeking to unlock development outcomes through inclusive financial services and the financial sector more broadly.
For more info, visit **www.cenfri.org**.

About FSD Africa

FSD Africa is a non-profit company that aims to increase prosperity, create jobs and reduce poverty by bringing about a transformation in financial markets in sub-Saharan Africa (SSA) and in the economies they serve. It provides know-how and capital to champions of change whose ideas, influence and actions will make finance more useful to African businesses and households. It is funded by the UK Aid from the UK Government. FSD Africa also provides technical and operational support to a family of 10 financial market development agencies or "FSDs" across SSA called the FSD Network. For more info visit **www.fsdafrica.org**.