Assessing the Role of Biometrics in Advancing Financial Inclusion

VISA

Executive Summary

Biometrics technology has received widespread attention as a means of enhancing convenience and security of digital payments. Many observers have highlighted potential benefits of using biometrics technology to advance financial inclusion.

This paper analyses how, and under what conditions, biometrics can facilitate access to and usage of financial services for lower income and unbanked populations. It examines the technology's potential and its present limits to advancing financial inclusion. The paper also highlights the policies and regulations that are necessary to enable biometrics to play a beneficial role in financial inclusion.

Introduction

Measuring biometrics against five key features of financial inclusion (convenience, trustworthiness, accessibility, affordability, and usefulness) indicates that the technology holds considerable potential for helping to reach unbanked populations. Biometrics may enhance convenience of financial services, for instance by reducing reliance on cards, PINs or passwords. They may improve trustworthiness, by re-assuring account holders that they have sole access to their accounts – an especially important issue for women. In some cases, biometrics may help make financial services more accessible for marginalized populations by providing solutions to those with limited access to identity documents. Where biometrics are tied to a centralized identity or biometric database, they may help make it more affordable and thus scalable for financial service providers to reach the under-banked.

At the same time, deployment of biometrics can present challenges or trade-offs. For instance, biometrics can be expensive to deploy, with a high cost for providers to enroll customers, and to record and store their biometric data. Intermittent connectivity in regions with limited infrastructure and hardware failures due to dust and humidity can challenge reliability, and thus confidence in the system. And, users around the world are increasingly concerned about privacy, security, and control over their data.

As governments, industry players, international organizations, community groups and others come together to advance financial inclusion, stakeholders may come to different conclusions about the optimal role for biometrics in supporting financial inclusion objectives in specific contexts. Yet, biometric solutions play a beneficial role in leveraging technology to help address persistent and emerging challenges in financial inclusion. Cross-sector dialogue on these challenges and opportunities can help smooth implementation of potential solutions and provide avenues to explore public-private partnerships to meet the needs of unbanked populations.

The term biometrics refers to the unique, intrinsic characteristics that can be used to identify or verify the identity of an individual. Biometrics are categorized as either physical or behavioral. Physical biometrics are individual biological or physiological traits such as fingerprints, facial characteristics, and iris patterns. Behavioral biometrics are traits that describe how individuals operate or function, such as a person's keystroke patterns or gait.

Terminology

Visa's definition of financial inclusion is that everyone, everywhere is able to use secure, convenient and affordable payment and financial services to meet everyday needs and long-term goals.

This definition rests on five key features:

Convenience - Once an underserved consumer accesses an affordable and useful financial service, it must be convenient to activate and continue using. This typically means that financial services must be available to consumers during their normal routine and require only minimal time to maintain.

Trustworthiness - Financial services must provide a basic level of security and an assurance of privacy to support ongoing trust and financial value.

Accessibility - Financial services must be readily available. Individual consumers and business owners must be able to reach a financial service and use it with the knowledge and tools they already possess or can easily obtain.

Affordability - Financial services for unbanked populations must be relatively affordable when compared to existing options such as cash, bartering, and traditional forms of credit and insurance, while offering providers a rate of return that facilitates sustainability and investment.

Usefulness - While local context and cultural norms are important considerations, generally the financial needs of the unbanked are no different than those of the banked. These needs include the following: ability to make payments, means to save, capacity to acquire credit, and mechanism for insurance.

Biometrics for Financial Inclusion

Based on current applications, biometrics technology is serving as a useful tool to support the five criteria for financial inclusion.

Convenience

Biometrics can enhance the convenience of financial services. For those who are new to the use of formal financial products, using familiar and intuitive biometrics like fingerprints can help foster comfort with financial transactions. Applying the finger to a scanner can make formal due diligence processes feel less foreign or alienating, compared to having to present a formal identity card for inspection or a signature for review. Biometrics can help populations with low levels of literacy better navigate typical financial processes, for example reducing the instances of written forms to be completed.

Inconveniences such as resetting forgotten passwords or exposed PINs can quickly become major barriers, and are eliminated with biometrics. Biometrics may also be appealing to young people, who are often more tech-savvy than other segments of the unbanked population, and may help draw them into the formal financial sector.

Biometrics, however, may themselves impose barriers to some of the very population financial inclusion seeks to serve. For low income people who are day laborers and farmers, degraded fingerprints may make the most common biometric identifier unavailable to them. Older people may experience similar degradation of fingerprints. Biometrics may also impose barriers for populations with physical limitations, e.g., impaired eyes and fingers with limited mobility. Providing consumers with multiple authentication choices, such as secondary biometric modalities and/or more traditional authentication mechanisms[1], can help accommodate users with special needs.

Convenience and use can be further enhanced by tailoring biometric systems to the desired user population and geography, e.g., including local dialects in voice recognition systems, and ensuring facial recognition algorithms include female features and skin tones of minority groups. Tailored approaches like these can help improve financial inclusion by broadening the user base, including under-represented groups and communities.

[1] "Biometric Authentication in Payments: Considerations for Policymakers." Promontory Financial Group. November 2017. http://promontory.com/payment_biometrics/

Trustworthiness

Biometrics can increase trust in the formal financial ecosystem among under-banked populations. A biometric identity is attached to an individual in a way that no other form of identification can be: it cannot be lost or forgotten. Moreover, people of all economic and educational levels share an intrinsic understanding that biometrics are inherent to who an individual is – for example, my fingerprint is me. This basic fact can create trust in a process, even if the process is new or not well understood.

Use of biometrics may also help make moments of authentication or access less susceptible to cultural or legal discrimination against certain populations, as may occur when a bank teller, financial service provider, or official reviews a piece of identification that reveals name, gender, address or, in some cases, ethnicity.

Another aspect of trust stems from security and privacy. In some situations, biometrically-based access can offer consumers increased privacy, ownership security, and protection of their financial assets – which may incent account opening and confer other socio-economic benefits. This can be especially beneficial for women in certain socio – cultural contexts. For example, biometrics can empower and protect women in situations when customs dictate that a man has a right to his wife's property, or that of a relative's widow. Because biometrics are tied to a particular individual, they can aid providers in protecting account privacy, even in the presence of adverse societal or communal pressures.

As part of a layered, risk-based approach to payments security, biometrics can help ecosystem players enhance security while reducing friction at the point of sale. With risk-based authentication, ecosystem players may choose to take a selective or segmented approach; instead of requiring all transactions to be actively authenticated, irrespective of their characteristics, advanced authentication (such as biometrics) may be reserved for the small proportion of transactions that look suspicious. Low-risk transactions may require more limited authentication, removing friction and creating a more seamless customer experience. This approach allows financial system entities, including those that target unbanked populations, to focus limited resources on transactions with the greatest risk.

At the same time, trust-related considerations around the use of biometrics are complex. For example, while individuals may be open to providing biometric information for enhanced convenience, they may be uncomfortable with a requirement to share this same data. This has implications when enrollment of biometrics in a state-run digital identity program is a requirement for receipt of social services and other benefits. It may also be a concern if the request comes from a private provider that does not provide consumer choice or alternative identification means.

Additional considerations around trustworthiness include: where biometric data is stored (in a centralized repository such as at a bank or government agency, or in a decentralized location such as on a consumer card); who is responsible for the security of that data; what information is transmitted to whom and when; and, how consumer consent is obtained.

For some users, local biometric storage on a card or device is an attractive alternative to centralized storage as it provides users with more direct control over their biometric data. Yet, this approach has trade-offs for costs, and can raise other data storage and security issues. Other individuals may have questions about security while using biometrics, e.g., questions around spoofing, or trying to fool a biometric authentication system using a fingerprint replica, facial photo, or other mimicked biometric. The biometrics industry is investing in a variety of techniques to make it harder for fraudsters to spoof a fingerprint, photo, or voice and use it to commit fraud. For example, cameras are now capable of registering micro-movements to distinguish between a real user and a photo of the user. "Liveness" checks are available or coming to many biometrics systems. Continued investments in this area can help to mitigate fraudulent usage and also increase trust in biometric systems.

Case Study: Opportunity International in Malawi

Opportunity International, one of the first organizations to roll out biometrics-supported banking for low-income customers, has facilitated fingerprint-based customer registration and verification in Malawi since 2003. Following the product launch, Opportunity International noted an uptick in women opening accounts.

At one point, Opportunity International reported a client base that was approximately 84 percent female, far greater than the female participation rate for the overall financial system.[2] And, while the cost of the product was relatively high for the consumer, Opportunity International came to understand that the privacy and trust engendered by biometrics played an important role in the product's success, and reach to unbanked people.

The account cards issued to customers incorporated biometric fingerprint verification. This enabled local bank tellers and managers to resist peer and communal pressure to provide male relatives with access to women's accounts, and assured women that they had full ownership of their savings. This also removed some of the barriers for clients with low levels of literacy and numeracy since the fingerprint verification replaced other common forms of verification such as a written signature or a pin number.

For the bank, incorporating biometrics was complicated by connectivity issues, hardware degradation, and the lack of a national digital identity program. All of these increased costs for Opportunity International, highlighting factors that affect scale and sustainability, and could discourage other entities from offering similar products in other markets.

[2] Based on discussions between Visa staff and Opportunity International representatives in May 2018.

Accessibility

Meeting financial industry identity due diligence requirements can be time-consuming and complex for consumers, who may be asked to provide multiple forms of identity or to document identifying elements such as physical address or birth records. These requirements can be particularly challenging for marginalized populations and/or itinerant communities.

Biometrics can make financial services more accessible to individuals when financial service providers are able to tap into a centralized database of biometrics information to verify a customer's identity. Biometrics can also help to temporarily provide a solution for incomplete or missing identity documentation. For example, biometrics can help create a single, continuous identity by acting as a benchmark against which existing records, once recovered, can be compared.[3] In this way, biometrics may provide unique identification for refugees who have lost access to some or all of their documentation in the process of being displaced.

Typically, during enrollment, biometrics are registered and linked to a formal identity. Biometrics are not used to register an identity – you are you – in the first place, which is defined by national law. Especially where serious concerns about security or fraud exist, biometrics are generally not accepted as sole proof of identification.

Terminology

Enrollment is when biometric data is initially collected and registered and linked to a formal identity.

Identification is when biometric data is compared to enrolled data (previously associated with an identifier) to establish the identity of an individual.

Authentication refers to the process of using a previously established identity to validate that an individual is who he or she claims to be. These terms are increasingly important to financial services, given the advent of Know Your Customer (KYC) requirements as a tool for countering money laundering and the financing of terrorism.

Case Study: United Nations High Commissioner for Refugees (UNHCR)

The UNHCR has developed a biometric identity management system to re-establish and preserve identities among refugees. It reports that linking biometrics to UNHCR's existing registration data not only improves efficiency, but also mitigates against refugees' personal identities being lost, registered multiple times, or stolen.[4] UNHCR is also using biometrics as a method to re-establish identity – a prerequisite for accessing financial services as well as receiving aid benefits – in cases where displaced individuals have otherwise lacked a formally registered identity or documentation, and were previously registered by UNHCR.[5]

[3] Gelb, Alan and Anna Diofasi Metz. *Identification Revolution: Can Digital ID Be Harnessed for Development? Center for Global Development.* 2018. https://www.cgdev.org/publication/identification-revolution-can-digital-id-be-harnessed-development

[4] "Biometric Management Identity System: Enhancing Registration and Data Management." UNHCR. 2015. http://www.unhcr.org/550c304c9.pdf

[5] "Biometric Management Identity System: Enhancing Registration and Data Management." UNHCR. 2015. http://www.unhcr.org/550c304c9.pdf

Affordability

Customer identity verification is fundamental to maintaining security and trust in the financial services ecosystem, but it is also a significant cost to financial service providers. These costs can be important considerations for providers evaluating products for low-income customers as these products typically have tight profit margins and target audiences who are not able to absorb sizeable pass-through costs.

Where there is a centralized repository of identity information that includes biometrics, biometric authentication can shift or reduce the cost of identity verification, leading to lower-cost financial services for consumers. Typically, a national government operates this type of centralized database, and permits trusted third parties such as financial service providers to verify a customer's identity using his or her biometric data. Whether publicly or privately run, a centralized identity database can reduce total costs by eliminating expensive duplicate enrollment processes. It may also redistribute costs from financial service providers to a government, or enable the sharing of costs among public and private entities. This redistribution or sharing of costs may improve the economics of designing and delivering products that reach underserved populations. Not all countries have national identity programs, however, and not all include biometric information, with governments deterred by the cost of enrolling biometrics information, security challenges, privacy considerations, and other factors.

Governments use biometric authentication in diverse programs, such as to deliver social benefits or pensions, because it can reduce fraud and delinquency, lower costs, and enhance efficiency. For example, according to the CEO of the South African Social Security Agency, the requirement for biometric authentication for delivery of benefits resulted in the "elimination of ghost accounts, duplications, and other irregularities…creating annual savings of approximately US$157 million."[6]

Program design can also affect affordability. Creating a closed loop system to enroll and store biometric information may provide a government agency or financial service provider with a quick way to implement a new program. However, the sponsoring entity bears the total cost, without the benefit of economies of scale offered by a shared database. This design may affect the affordability of program-issued products and services. If the program requires that biometric information be stored on a card, a set-up that can be advantageous in locations with unreliable connectivity, the expensive enrollment process must be repeated each time a card is lost.

Finally, use of biometrics introduces different operational costs to ecosystem players. For instance, in the experience of Opportunity International (OI), an organization that provides financial solutions and training to low-income populations, physical infrastructure related to the use of biometrics is relatively affordable (OI has used small devices that can be plugged in to existing terminals), but highly durable devices that can withstand heavy use or extreme conditions are more expensive.[7] Outreach to consumers, connectivity, training, and additional staff all add to costs.

[6] Riley, Thyra A., and Anoma Kulathunga. 2017. Bringing E-money to the Poor: Successes and Failures. Directions in Development. Washington, DC: World Bank. doi:10.1596/978-1-4648-0462-5. License: Creative Commons Attribution CC BY 3.0 IGO http://documents.worldbank.org/curated/en/340701503568346911/pdf/119070-PUB-PUBLIC-PUB-DATE-8-22-17.pdf

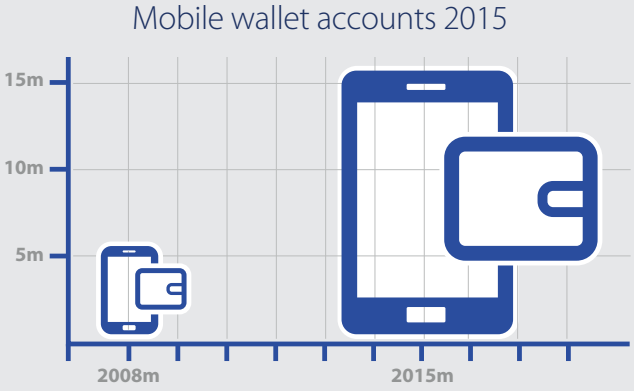
[7] Based on discussions between Visa staff and Opportunity International representatives in May 2018.

Usefulness

Biometrics may contribute to the overall usefulness of financial services to an underserved consumer or small business owner. Usefulness refers to how well a product meets the needs and underlying goals of the user: for example, the ability to make payments without leaving one's self-run store or standing in line for hours; safely saving for school fees; securing long-term financing to invest in a business; or, obtaining insurance to protect against frequent flooding of crops.

Usefulness is typically achieved in the design of the product or service itself. However, over time, a common, secure biometric authentication process might be leveraged as an efficient way to migrate consumers or small businesses from low value products to higher value services that meet their long-term goals (such as long-term financing) with minimal transaction costs or requirements.

Case Study: Pakistan's National Database and Registration Authority



In Pakistan, the National Database and Registration Authority's (NADRA's) risk-based, tiered approach to regulations around bank account opening and its collection of biometric information helped pave the way to a more convenient account opening process.

Starting in 2008, Pakistan's NADRA began to collect fingerprints of individuals registered with the national identity program. NADRA's use of biometrics made account opening more convenient for consumers thanks to branchless banking regulations that required only a biometric fingerprint scan at agent locations, instead of a branch visit, to open the lowest level mobile wallet. These regulations were revised in 2016 to allow users the ability to establish a mobile wallet account through a biometrically verified SIM authenticated by the NADRA database.

In 2015, the total number of mobile wallet accounts tripled from 5 to 15 million, with approximately 50 percent of new registered mobile wallet accounts opened using biometric authentication.[8]

[8] Rashid, Naeha and Stefan Staschen. "Unlocking Financial Inclusion Using Biometrically Verified SIMs," Consultative Group to Assist the Poor (CGAP) Blog. July 26, 2016. This translation was not created by CGAP and should not be considered an official translation. CGAP shall not be liable for any content or error in this translation. www.cgap.org/blog/unlocking-financial-inclusion-using-biometrically-verified-sims

Policy Enablers

The following policies and regulations can enable biometrics to play a beneficial role in advancing digital payments and financial inclusion in sustainable, scalable and responsible ways, alongside other national goals.

1 National and Digital Identity Frameworks

Biometrics hold potential to advance financial inclusion, but depend on a national legal identification framework to answer the primary question of 'who are you' to which biometrics are then tied. Policymakers can enable biometrics to help advance financial inclusion and social welfare goals by strengthening the national identification framework so that it covers all citizens, if it does not already do so. Including possibilities for self-identification or peer-identification in specific, limited circumstances can boost financial inclusion possibilities among populations who lack formal birth records or permanent addresses, for example. Establishing multiple 'on ramps' for citizen enrollment in a biometric registry is also helpful.

Shared registries of identity information, including biometrics, may reduce the costs faced by financial institutions in meeting their identity due diligence requirements, thus enabling the offering of low-cost products tailored to underserved people and businesses. There are various models, such as government run and federations including private sector. In these and other models, allowing trusted financial service providers access to the database eliminates the need for each provider to establish their own proprietary database. This can improve speed and efficiency of account opening, and thus the overall experience for consumers. Combined, these factors can foster on-going innovation and interoperability, and help financial service providers reach scale more quickly.

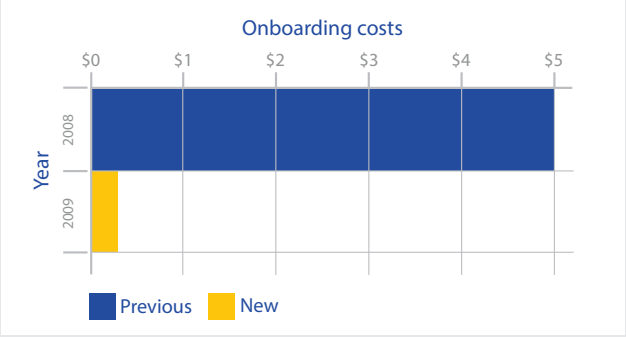
2 Data Security and Privacy Policies

Policymakers can further support the benefits of biometrics by strengthening their data security and privacy laws to increase confidence in the formal financial sector in general and in biometric usage specifically. Strong, harmonized standards and requirements on the ways in which public and private entities register, store, secure, transmit, manage and share biometric data can help avoid unintended negative consequences in the provision of financial services to low-income populations. For example, what data needs to be shared and transmitted to achieve identity verification goals? Would sharing an assertion of a data match be sufficient to meet authentication goals instead of sharing actual biometric data? Industry-led standards for secure data storage and transmission, developed with cross-sector input, can improve security practices for handling consumer data while enabling interoperability (i.e., the ability of systems or devices to exchange information and operation in conjunction with each other).

Harmonized, global standards can also encourage interoperability and reduce costs. Such standards do not necessitate a certain form of biometric identification but instead require overall standards that ensure interoperability, privacy, and security. Common standards can facilitate economies of scale, helping individual providers feel confident in receiving financial returns on their investments and therefore encourage the creation of new and innovative biometric-enabled products.[9] Implementing already-established global standards can increase efficiencies, ease the burden on domestic entities to create and maintain their own standards, and ensure interoperability across national borders. By leveraging global standards, domestic investment can support more local product development and financial inclusion efforts.

[9] "Biometric Authentication in Payments: Considerations for Policymakers." Promontory Financial Group. November 2017. http://promontory.com/payment_biometrics/

Case Study: India's Aadhaar



By some estimates, services of Aadhaar, India's identity database launched in 2009, have reduced the cost of onboarding a customer from around US$5 for commercial banks to US$0.07 for the new "payments banks" set up to increase financial inclusion.[10] These figures indicate that, through Aadhaar's biometrics, some financial institution operational expenses have been transferred to the government, offsetting costs for banks and changing the economics of expanding their reach to the financially excluded.

However, the savings from Aadhaar remain contested. Banks and other entities must pay a fee to use Aadhaar's authentication services, and some banks - particularly small ones serving low-income, rural populations - have issued complaints arguing that these fees are not affordable.[11]

3 Telecommunications and Financial Infrastructure

Extensive, reliable infrastructure is key to advancing financial inclusion and social impact through digital means. Using biometrics generally requires robust infrastructure including electricity and internet or phone connectivity with wide coverage. For example, biometric scanners may require electricity connection or battery power. Connecting to a centralized identity database to authenticate biometric information typically requires communications connectivity. Erratic, slow, or expensive connectivity can discourage usage. A number of innovative products have been designed to overcome the lack of reliable electricity and connectivity. These include products that store biometric information on a beneficiary or consumer card. During a transaction, scanned biometric information is compared to the verified data stored on the card. While effective, this approach has trade-offs in terms of costs and ease of use.

Beyond the cost of establishing a common registry there are many infrastructure costs associated with biometric identification and authentication. Examples include: upgrades to point-of-transaction terminals to enable biometric data capture, dissemination of secure cards that store biometric data, and maintenance of reliable connectivity between a central identity registry and individual financial service providers.

As the cost of these requirements is compounded in rural settings, investments that improve the overall infrastructure of a country may support greater adoption of biometric-based identification systems and greater financial inclusion.

4 Government Use and Promotion

Policymakers can increase the scale of biometric authentication by tying certain government services to centralized identity databases. For example, many of the most impoverished individuals rely on government or international agency aid to meet their daily needs. A number of governments have already introduced biometric verification as a requirement to receive such benefits. This can help introduce consumers to biometrics and financial services, and can jump start the use of biometrics in markets.

The design of such a program has implications for scale and cost, and the number of additional financial services that can be layered on to biometric-enabled accounts. Tying social and civic services such as voting, land and property registration, and mass transit ticketing to biometric authentication can further increase demand and scale. At the same time, linking core public services and benefits programs to biometrics could lead to exclusion if non-biometric options are not also available as an alternative authentication mechanism. Without multiple on-ramps available to establish one's biometric identity, those without access to such a system may find themselves further dis-enfranchised and marginalized.

[10] Gelb, Alan and Anna Diofasi Metz. *Identification Revolution: Can Digital ID Be Harnessed for Development?* Center for Global Development. 2018. https://www.cgdev.org/publication/identification-revolution-can-digital-id-be-harnessed-development

[11] Saha, Manojit. *"Banks baulk at high cost of Aadhaar verification." The Hindu.* June 16, 2018. https://www.thehindu.com/news/national/banks-baulk-at-high-cost-of-aadhaar-verification/article24175437.ece

5 Consumer Protection

Strong laws and regulations that protect an individual's right to his or her account and biometric data are essential. At the user level, individuals, particularly women in countries with a history of patrimonial control, need to be confident that their relatives or others will not be able to access their savings or conduct transactions without their consent. The very personal and individual nature of biometrics can enhance certainty in this area. Even this powerful technology must be backed up with a sound legal framework and trustworthy jurisprudence.

Regulations to ensure consumer protection, such as requirements for clear disclosures, can help avoid unintended negative consequences in the provision of financial services to low-income populations. By anticipating implementation challenges, policymakers may be able to avoid creating an inequitable situation in which traditionally underserved populations are forced to surrender a level of privacy enjoyed by more advantaged populations.

6 Proportional, Risk-Based Financial Regulations

Creating proportional regulatory frameworks around Know Your Customer (KYC) requirements can help to protect the financial ecosystem, while also supporting financial inclusion goals. Traditional KYC verification requirements such as multiple forms of identification and proof of a physical address are often difficult for low income, unbanked and marginalized individuals to provide. Implementation of a tiered KYC regulatory framework can enable individuals to open a simple – yet formal – transactional account with basic identity information.

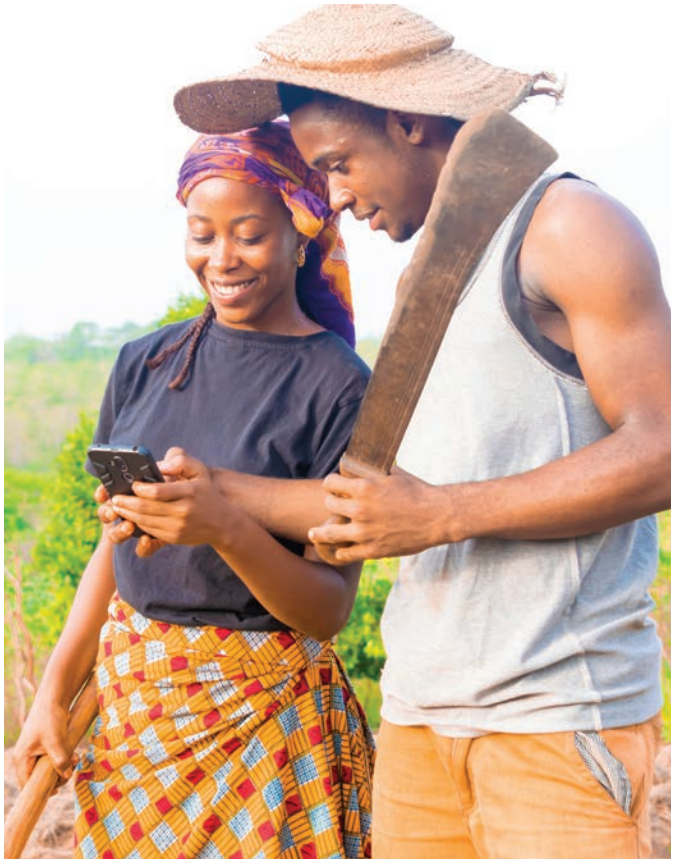
The simplest tier of basic accounts may permit a tailored threshold of initial identification to obtain a prepaid card or open an account. In exchange, they may incorporate a low maximum account balance and limited monthly transactions, parameters which are typically sufficient to meet the relatively basic needs of the previously unbanked. In fact, allowing for a zero initial balance can help achieve maximum accessibility.

In some cases, governments may allow an unbanked individual to open a limited transaction account throughan agent, presenting just a fingerprint or iris to establish identity. In other cases, financial service providers may leverage a centralized identity registry to verify the identity of a new customer. Within tiered KYC frameworks, biometrics are a tool that banks or governments can incorporate toease and expedite onboarding processes – especially for lower-tier accounts geared toward low-income and unbanked individuals.

7 Branchless Banking, Mobile Money and Other Innovations

Biometrics are often most effective in supporting financial inclusion when combined with other innovations such as branchless banking and mobile-based banking, as well as banking through post offices. With supportive regulations, financial service providers may enable agents to use biometrics as a secure, convenient method for authenticating consumers, further driving reach and scale.

Allowing different models of branchless banking provides flexibility for local providers to develop market-appropriate solutions. Encouraging new entrants in the financial services area, such as financial technology (fintech) firms or other service providers, can help expand the types of solutions available to underserved populations. This may merit some initial regulatory flexibility, commensurate with associated risk. More generally, ensuring that non- financial institutions and new entrants offering branchless banking are subject to the same prudential regulations as financial institutions can provide consumers with a baseline of security and protections across the ecosystem. Looking ahead, systems that use biometrics in conjunction with other emerging technologies may offer further potential to build scale.



8 Training and Financial Literacy

Some low-income, under-banked populations have low levels of financial literacy, which can act as a barrier to participation in the formal financial system. Educational efforts among consumers, merchants, financial institutions, technology providers, and independent agents are critical – especially for micro and small merchants who often provide points of access for low-income consumers. Training in using biometric readers – via smart phones, dedicated readers, ATM adaptors, or other devices – can support adoption from a practical sense. Educating consumers on methods to use and protect their biometric data can help grow trust in new forms of authentication.

9 Political Leadership and Coordination

Political leadership is critical to successfully leveraging biometrics to increase financial inclusion. Because scale is so important for the ultimate success of biometrics to achieve greater financial inclusion, coordination across government agencies can help maximize investment, leverage existing human and physical infrastructure, build interoperability, and avoid competing standards. Addressing biometric usage and program design as part of national financial inclusion strategies or policies can also help drive expanded use.

Case Study: South Africa's Social Grant Distribution Program

In 2012, the South African Social Security Agency (SASSA) consolidated multiple systems for distributing social grants into a centralized program. As part of the consolidation, the SASSA reregistered recipients with their biometrics. Outside observers noted that the use of biometrics helped to reduce fraud and delinquency,[12] but in some cases, the financial products offered through the grant delivery system reportedly did not align with the financial goals of the targeted population. Thus, while effective at eliminating fraud, incorporating biometrics did not automatically address the usefulness of the underlying products (e.g., product design and delivery).

Conclusion

Biometrics technology holds sizeable potential as a tool to advance financial inclusion, contributing to the convenience, trustworthiness, accessibility, affordability, and usefulness of financial services for underserved populations. However, biometrics are not a stand-alone solution to all financial inclusion challenges. Considerations around consumer protection, infrastructure, and other issues factor into individual government decisions about how and when to leverage biometrics to drive financial inclusion forward.

The practical application of biometrics to the financial ecosystem is built on a complex foundation of policy enablers. Biometrics can be most impactful when incorporated as part of broader financial inclusion strategies, and in contexts where governments take a principles-based, innovation -friendly approach to regulation and policy making.

[12] Gelb, Alan and Anna Diofasi Metz. *Identification Revolution: Can Digital ID Be Harnessed for Development?* Center for Global Development. 2018. https://www.cgdev.org/publication/identification-revolution-can-digital-id-be-harnessed-development

