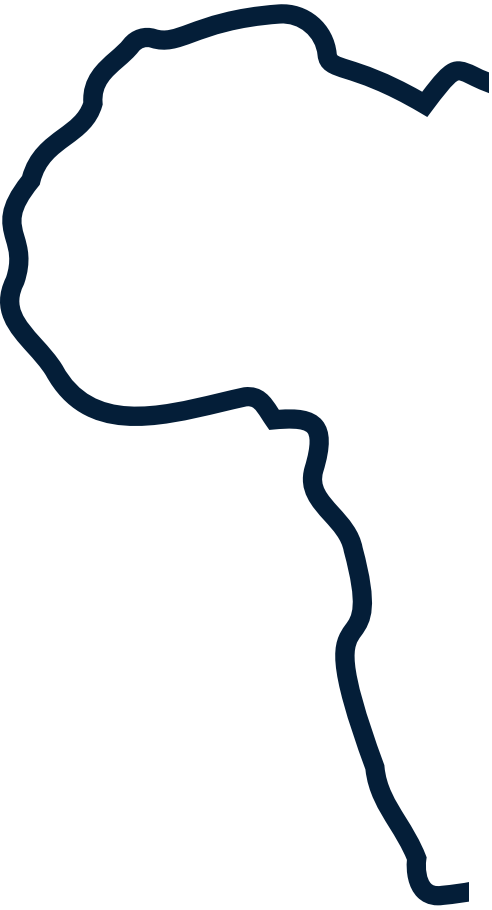
iiDENTIFii
Remote Biometric Identity Authentication



WHITE PAPER

BIOMETRIC AUTHENTICATION IN AFRICA: NAVIGATING THE DYNAMIC THREAT LANDSCAPE IN 2024

JANUARY 2024

In Africa, market-specific threats such as SIM swap fraud and online banking-related kidnappings are continually evolving to circumvent digital safety measures. In addition to a potentially positive impact on safety, a secure digital identity also holds the potential to revolutionise elections, financial services, and overall economic inclusion on the continent. In order to achieve this, IDV (Identity Verification) providers have to focus on relevant, diverse algorithms that counteract bias and accessible, enterprise-grade technology that stands up to rapid expansion and constantly evolving security threats.

Africa is a sleeping giant and the requirement for digitised biometric authentication is immense. If we can scale effectively across the continent and continue to counteract continually evolving cybercrime threats, IDV has the potential to have a powerful and sustainable impact. This paper explores some of the trends in Africa's threat and opportunity landscape.

Key insights

- What are the main biometric authentication threats in Africa?
- What are the key opportunities to counteract these threats?

Threats

SIM swap fraud

South Africa's mobile service providers continue to face pressure from new and existing clients to tighten up their data security, as fraudsters continue to take advantage of false identities and SIM swap scams.

The last few years have seen a sharp rise in SIM swap fraud, placing the mobile and digital sectors at risk of disrepute. In 87% (9 571) of the mobile banking fraud incidents reported to the South African Banking Risk Information Centre (Sabric) in 2020, SIM swaps were part of the modus operandi. These increased to 93% (19 730) in 2021. The number of incidents involving SIM swaps increased from 2 686 incidents in 2020 to 4 386 reported in 2021, according to the report.

On a larger scale, the use of advanced technology and machine learning can automate the fraud process allowing fraudsters to conduct SIM swaps much faster and quickly identify vulnerable targets. The stakes in Africa are high, as SIM swap fraud negatively impacts the trust between mobile users and their mobile providers due to the substantial volume of data in their possession. This is even more important in cases of post-paid users, or jurisdictions with mandatory prepaid SIM card registration.

Advanced tech and machine learning

can automate the fraud process allowing fraudsters to conduct SIM swaps much faster

93%

of mobile banking fraud incidents in 2021 were SIM swap fraud

Threats

ID theft cases and kidnapping

While SIM swap fraud remains a threat across the continent, another concerning trend has emerged in South Africa: victims are being kidnapped and coerced to make transfers from their banking apps.

This overrides all the usual biometric protections in place, as the victim is forced into using their defining biometrics to log into and drain their own bank account. Criminals are operating under different syndicates, either targeting specific business owners or conducting attacks that are more opportunistic in nature.

This trend is supported by Sabric's Annual Crime Stats 2022 report, which noted that other types of mobile banking crimes were in decline while banking app fraud cases have increased by 36%. This suggests that, as the previously popular SIM swap method is proving less effective than in the past, criminals are migrating to banking app shakedowns.

The previously popular SIM swap method is proving less effective than in the past

Criminals are migrating to banking app shakedowns

36%

increase of banking app fraud cases, Sabric's Annual Crime Stats 2022

Threats

The Generative AI and voice-cloning shakeup

Voice cloning is another threat on the rise. Also known as 'deepfake voice', this refers to a criminal creating a cloned voice sample that mimics a person's speech using the power of generative AI.

This has dire implications for voice banking and the use of a biometric voiceprint in authentication. The technology required to impersonate an individual has thus become cheaper, easier to use, and more accessible. This means that it is simpler than ever for a criminal to assume one aspect of a person's identity.

In the United States, for example, the Federal Trade Commission issued an alert urging consumers to be vigilant for calls in which scammers sound exactly like their loved ones. All a criminal needs is a short audio clip of a family member's voice – often scraped from social media – and a voice cloning program to stage an attack. This is relevant to Africa too. According to the Southern African Fraud Prevention Service (SAFPS), impersonation attacks increased by 264% for the first five months of the year compared to 2021. As voice-cloning becomes a viable threat, financial institutions need to be aware of the possibility of widespread fraud in voice-based interfaces and counteract it with sophisticated and multi-layered biometric authentication processes.

It is simpler than ever for a criminal to assume one aspect of a person's identity

The technology has become cheaper, easier to use, and more accessible

264%

increase of impersonation attacks for the first five months of 2022 compared to 2021

Opportunities

Providing inclusive identification in Africa

Biometric identity does not just protect consumers from threats. It offers a new landscape of identification, where access is opened up for a world of essential services for those for whom it was previously out of reach. An inclusive digital identity approach can open doors to critical government services such as labour markets, government benefits and financial services, without the risk of impersonation or fraudulent funding. This extends to those with limited ability to engage in the digital world.

Historically, proof of identity was only available to those who could fulfil a rigid set of criteria. One of the main barriers to a person opening a bank account, for example, would be the inability to prove their identity without any formal identity document or proof of formal address. According to the World Bank, 57% of Africans still have no bank account, including mobile money accounts. A recent study by BPC and Fincog found that this translates to about 360 million adults in the region and approximately 17% of the total global unbanked population without access to formal financial services. According to McKinsey, extending full digital identity coverage could unlock economic value equivalent to 3-13% of GDP by 2030.

57% of Africans
still have no bank account, including mobile money accounts

The World Bank advocates for
the development and deployment of Digital Public Infrastructure (DPI)

Biometric identification
is among four aspects fuelling migrant instrumentalization

Recently, a group of the 19 most advanced economies in the world, the European Union, and most recently the African Union, the G20, published a policy guide in partnership with the World Bank advocating for the development and deployment of Digital Public Infrastructure (DPI) to advance financial inclusion and productivity gains in the Global South. IDV providers have an important role to play in the implementation of an inclusive DPI as a safe and robust digital identity will enable citizens to access such systems.

The impact of inclusive biometric identity is already being felt. An academic study on migrants from five central and west African countries seeking refuge in Nigeria found that biometric identification is among four aspects fuelling migrant instrumentalization, especially for election purposes.

Opportunities

Biometric identity as an enabler in African elections

One of the greatest potential areas of inclusion will be elections, where remote biometric authentication can reduce duplication and improve the legitimacy of the election process. Both factors have a powerful impact on a sensitive process where a country's future leadership is at stake.

Nations such as Zimbabwe and Liberia have adopted biometrics for their upcoming elections, and countries such as Nigeria, Ghana, Sierra Leone, Cameroon, Namibia, Rwanda and the Democratic Republic of Congo are all actively implementing or planning to implement biometric authentication programmes across the country.

However, one factor stands in the way. Countries rolling out biometric programmes for the first time will encounter challenges if their solution is not anchored in a complementary infrastructure. In Liberia, for example, the biometric voter registration process was held up owing to delays in the equipment required for an effective rollout. In Zimbabwe's recent biometric registration, some civil society groups were concerned that the Zimbabwe Electoral Commission (ZEC) was not registering all who applied.

In reality, this happened because some citizens were already registered, and other registrations took place offline, so no confirmation was given. In the wake of the elections in Nigeria, some citizens feared that systems like the BVAS were a new tool for electoral fraud. Widespread public education is critical to the success of biometric authentication systems, especially in the context of elections. Even though the benefits far outweigh any perceived risks, using familiar technology such as selfie images, makes citizens far more comfortable with the technology platform.

Improve legitimacy of the election process

through remote biometric authentication

Public education is critical

to the success of biometric authentication systems

Opportunities

Biometrics for low-end smartphones

Inclusivity extends to infrastructure as well as the ability to access biometrics platforms on devices.

For example, someone with a lower-quality camera on their device may have a more difficult experience verifying their identity than a person with a more sophisticated device. Technology must perform well for both groups or it risks being biased. As banks, governments and other organisations consider identity verification solutions, it is important that they check that vendors can demonstrate robust bias mitigation and compliance with WCAG and other accessibility standards.

At present, iiDENTIFii is proud to be the only IDV that can operate on mobile devices that aren't smartphones.

Bias and diversity in biometrics

Historically, international biometric authentication and facial biometrics have carried bias in who they successfully identify.

In 2018, an MIT study found that three commercial facial analysis programs had a margin of error between 20% and 34% when identifying dark-skinned women, compared to 0.8% or lower for light-skinned men.

iiDENTIFii is the only IDV that can operate

on mobile devices that aren't smartphones

Over 50 million African faces

have trained the iiDENTIFii algorithm

The same study indicated the root cause for this – the facial data used to train at least one of the systems was more than 77% white and more than 83% male. Another study by the National Institute of Standards and Technology (NIST) found that facial recognition algorithms falsely identified African American and Asian faces 10 to 100 times more than Caucasian faces. Facial biometrics will be less able to identify the patterns found in a particular demographic's faces if the initial data sets it was trained on did not contain a diverse range of faces from a wide variety of demographics. Simply put, facial biometrics can't pick up a pattern that it hasn't seen before.

Because every person has the right to identity and to be positively and easily identified, IDV systems need to ensure that the datasets used to train algorithms are balanced according to age, gender, and skin tone. With this in mind, iiDENTIFii's algorithm has been trained on over 50 million African faces to make it relevant to our continent.

Opportunities

Governance of biometrics

As biometrics becomes an influential technology across the continent, there will be an increasing need for the design of robust governance frameworks.

The greatest challenge lies in developing these frameworks at the same pace as the widespread rollout and evolution of digital identity systems. These systems need to be inclusive, trustworthy, and reliable as well as involving both public and private sector stakeholders.

As Sarah Lister, head of governance at the Bureau for Policy and Program Support at the United Nations Development Programme states, “Governance is the way a society organizes itself to make and implement decisions and to get mutual understanding, agreement, and action. Public participation and people’s confidence and trust are vital. Governance is not just about having the legal or regulatory framework; to make a regulation or a law work, you need to have a system of other elements that work together to create an environment in which the law or the regulation can be implemented.”

Embracing biometric authentication as a crucial shield against evolving threats in Africa

To champion digital and financial inclusion, companies and experts need to collaborate and provide solutions that reach consumers where they are and solve their unique challenges.

iiDENTIFii is committed to mobilising its uniquely African, enterprise-grade biometric identity solution to drive greater access to financial, health, education and citizen services across Africa

iiDENTIFii is an award-winning face authentication and identity verification platform that distinguishes itself through its use of 3D and 4D Liveness® detection.

iiDENTIFii is the only IDV that can operate

on mobile devices that aren’t smartphones

Purpose-built for enterprises across Africa and the Middle East, iiDENTIFii enables frictionless, scalable customer onboarding in seconds from anywhere and on any device. It makes use of non-invasive automated proven processes that meet customer intelligence, risk and compliance goals, as well as governance and legislative requirements. Founded in 2018, iiDENTIFii has become a proven key partner in multiple tier-1 African banks. The technology plugs seamlessly into existing infrastructures, including mobile and web-based platforms.

iiDENTIFii
Remote Biometric Identity Authentication

CONTACT US

Book your demo request with one of our experts to get bespoke advice on a solution that's right for your business.

Book a demo

anthony@iidentifii.com www.iidentifii.com