



The State of KYC in Africa H1 2023

usesmileid.com



Contents

| | | | |
|-----------------------------------------------------------------------------------------|-----------|------------------------------------------------------------------------------------------------|-----------|
| KYC Report H1 2023 | 1 | Zambia | 39 |
| Unlock Digital Africa | 3 | Senegal | 40 |
| Building a trusted user base: Importance of identity Infrastructure in Africa | 4 | Cameroon | 41 |
| Key Takeaways | 6 | Côte D'Ivoire | 42 |
| Identity Verification Landscape in Africa: The Trends and Insights | 8 | Africa's Digital ID transition: Countries to watch | 43 |
| Scale: 75 million checks and counting | 9 | Fraud Trends Across Africa | 44 |
| Speed: Onboarding users faster than ever | 10 | The Big Story: Generative AI and Fraud | 45 |
| Inclusion: Closing the gender gap | 12 | Common Types of Fraud Attacks | 46 |
| Fraud: down, but not out | 13 | Fake ID documents | 46 |
| Verification is critical; collecting documents is not enough | 14 | Stolen ID information | 47 |
| Fraud trends across the four key startup markets | 16 | Selfie "Spoofs" | 48 |
| BNPL fraud rates drop significantly; Crypto and Payments are on the rise | 18 | Duplication Fraud | 49 |
| National ID database uptime is improving in 2023 | 19 | Synthetic Fraud | 50 |
| Some ID types experience more frequent downtimes | 20 | Business Registration Fraud | 51 |
| Foundational vs Functional ID document types | 21 | Secure your business: How identity verification helps companies prevent fraud | 52 |
| Country Deep Dives: KYC Compliance Across Africa | 22 | Document Verification: A critical tool for fraud prevention | 53 |
| The Big Story: South Africa, Nigeria & Cameroon now on FATF Grey List | 23 | Case Study | 55 |
| Nigeria | 25 | Biometric KYC for ID verification | 56 |
| South Africa | 27 | Why selfies are the go-to choice for biometric authentication | 57 |
| Kenya | 28 | Liveness checks using SmartSelfie™ | 58 |
| Ghana | 29 | Case Study | 59 |
| Uganda | 31 | Face Deduplication | 60 |
| Rwanda | 33 | AML Check | 61 |
| Tanzania | 34 | Know Your Business | 62 |
| Ethiopia | 35 | How to protect yourself from ID-related fraud | 63 |
| Egypt | 37 | | |

Unlock Digital Africa

Imagine a world:

that is safe, accessible, honest – and clear of fraud.

A digital economy rich in innovation and possibilities where technology services are accessible to everyone, and Africans everywhere are never excluded.

No boundaries, no closed doors.

Imagine a fast-growing economy: where business growth is not held back by redundant bureaucracy, nor is it threatened by duplicity. A world where digital trust is the norm.

That is the world that we believe in and are committed to building. At Smile ID, we are here to build and secure the infrastructure that unlocks Digital Africa and helps businesses build a trusted user base.



Building a trusted user base:

The importance of identity infrastructure in Africa



With over **54 countries** and **1.4 billion inhabitants**, identity infrastructure is pivotal in Africa's burgeoning digital economy, fostering financial inclusion and enhancing service delivery.

However, nearly 500 million Africans still lacked legal identity documentation as of 2020, as per the World Bank's ID4D Global Dataset, indicating a vast potential for identity verification solutions to bridge this gap.

Identity verification providers are especially vital in Africa's burgeoning fintech and banking sectors, where they can help mitigate fraud and enhance trust in digital transactions. The African Development Bank estimates that **Africa's digital economy** could reach **\$180 billion by 2025**, with secure digital identities being a cornerstone of such growth. McKinsey also forecasted that digital identification could unlock a value equivalent to 3–13% of GDP in 2030 for African economies, particularly in the finance, agriculture, and healthcare sectors.

Against this backdrop, we present Smile ID's H1 2023 State of KYC in Africa Report, offering insights into the critical role of Know Your Customer (KYC) processes & regulations in shaping the digital ecosystem.

As a pioneer and leading provider of identity verification solutions in Africa, Smile ID is uniquely positioned to offer insights into the evolving KYC landscape.

Our expertise, coupled with our extensive network spanning the continent, enables us to thoroughly examine the latest trends, regulatory developments, and fraud patterns in the African digital identity verification space.

In this report, we delve into the state of identity verification across various African countries. We also look closely at the fraud trends and how businesses can leverage identity verification to safeguard their operations.

We trust that you will find the insights in this report valuable as we navigate the evolving digital landscape together. As always, Smile ID remains committed to providing the most accurate, reliable, and inclusive identity verification solutions, enabling businesses across Africa to unlock the full potential of digital transformation.



Key Takeaways



Biometric verification reduces fraudulent users by 50%.

In 2023 so far, 43% of ID frauds caught were face mismatches indicating that stolen or lost IDs were used, while 41% were selfie spoofs.



Textual verification alone is insufficient for ID verification, as most fraudsters can only be identified through biometric checks.



Being the more accessible and secure option, facial recognition is the most preferred biometric KYC method worldwide.



ID databases remain critical infrastructure for real-time verification.

Local ID databases remain the most robust source of truth for KYC, but frequent downtime (on average 3%) remains an obstacle.



Document Verification ensures uptime during ID Database downtime.



It is also a better, more effective and more reliable way to launch in multiple markets with one integration.



Adoption of digital identity is growing across Africa.

Ethiopia begins enrollment for foundational Fayda ID.



Kenya to introduce Unique Personal Identifier to replace Huduma Namba.



Uganda to launch new digital ID scheme in Q4 2023.

Key Takeaways

3X% growth in female ID verifications in Africa

35%

Gender inclusion is growing on the continent with female ID verifications rising from 10% to 35% in the last 2 years.



BNPL leads the way in gender inclusion with an average of 30% female users over time-period.



Banking and Lending is the most improved industry, growing from 9% to 36%.

Onboarding fraud rates declined by 5% in focus markets, led by declines in South Africa and Ghana.



Over the years, incentive-based acquisition has had a high correlation with increased fraud attempt rates.

-5%

The 5% decline in fraud rates coincides with declining startup funding across the continent and has resulted in reduced marketing spend.

+7%

In contrast to others, Fraud in Kenya has increased by 7% over the last six months, with the National ID being the most attacked.

11 African countries are now on the FATF's grey list.



South Africa, Cameroon and Nigeria are now on the FATF's grey list joining countries like Uganda, Senegal, & South Sudan.

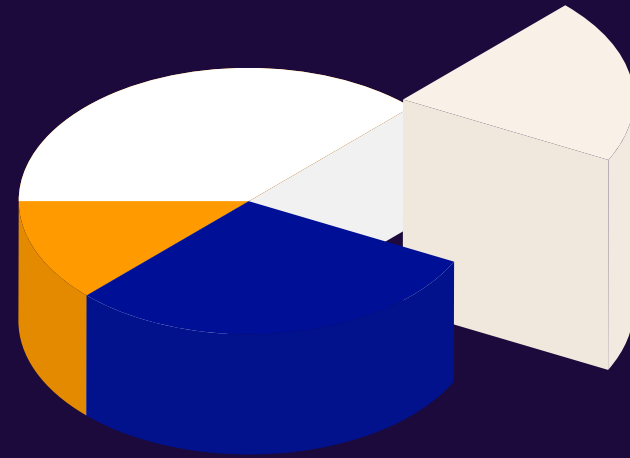


Regulations for accountable businesses are expected to evolve in the coming months.



Now more than ever, businesses across Africa must ensure their KYC/AML procedures are on par with international best practices.

Identity Verification Landscape in Africa: Trends and Insights



Scale: 75 million checks and counting

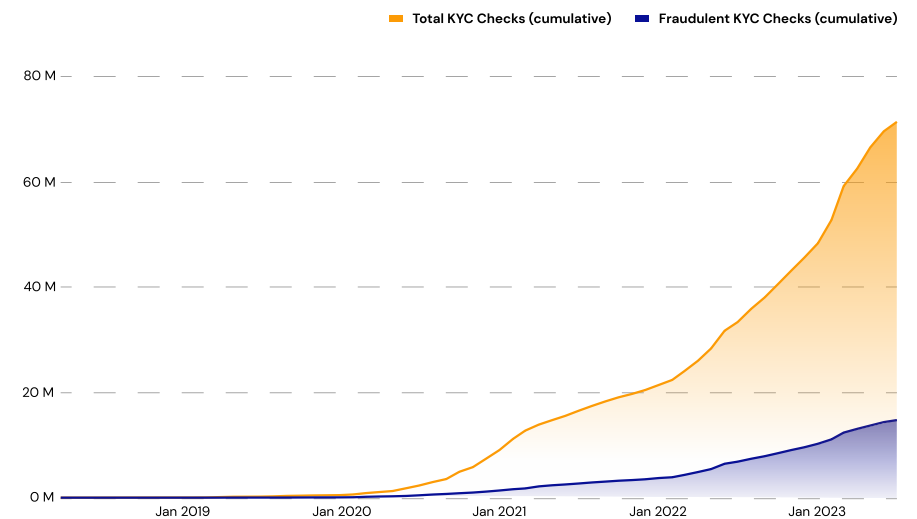
The first half of 2023 has seen African businesses embrace digital transformation with renewed vigour. As a result, the demand for accurate and seamless identity verification solutions has skyrocketed. We've witnessed this trend firsthand, having conducted over 75 million KYC checks since inception – an increase of over 50% in just six months.

Several factors drive this growth: the increasing adoption of digital platforms by businesses of all sizes, the growing importance of regulatory compliance, and the need to mitigate fraud.

Leveraging our expertise from previous years, in this report (our third), we deepen our exploration of KYC and digital ID trends and the impact of evolving regulations in Africa. As we progress through 2023, we remain committed to delivering the most accurate and reliable identity verification solutions, and we are confident that we will continue to play a vital role in enabling businesses on the continent to unlock the full potential of digital Africa.

KYC Checks by Smile ID

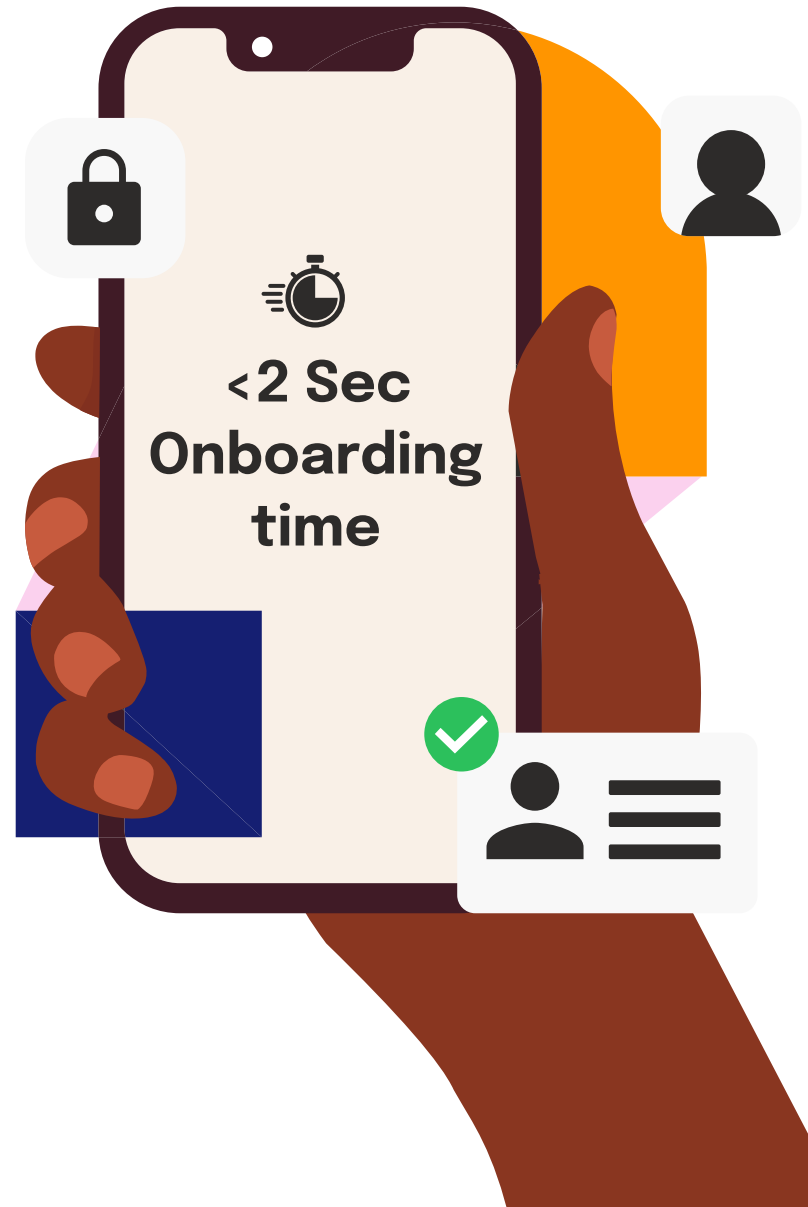
Cumulative checks over time



Note on chart and data set:

This report uses anonymised data collected from transactions on Smile ID. Fraudulent KYC checks include biometric fraud and data validation errors when checking against the government ID database. Data in this chart was collected from 2018 to June 2023.














Speed: Onboarding users faster than ever



In major markets such as Nigeria, Ghana, Kenya, and South Africa, Smile ID has reduced the average time for verification of the most popular IDs to a mere **1.93 seconds.**

This remarkable achievement allows businesses to onboard a vast number of users rapidly while meeting customer expectations for speed.

Furthermore, our coverage of the most popular IDs per country ensures that businesses can cater to a diverse range of users. In Nigeria, for instance, where businesses are allowed to open tiered accounts for users based on transaction and balance limits, Smile ID supports the recommended ID types for each tier, including Phone Number, Bank Verification Number (BVN), and National ID (NIN).

| Country | ID Type | Median Processing Time |
|------------------------------------------------------------------------------------------|-----------------------------------|------------------------|
|  NG | Nigeria NIN V2 | 2s |
|  NG | Nigeria Phone Number | 2s |
|  NG | Nigeria BVN | 3s |
|  KE | Kenya National ID | 2s |
|  ZA | South Africa National ID No photo | 1s |
|  NG | Nigeria Voter ID | 1s |
|  GH | Ghana New Voter ID | 1s |
|  UG | Uganda National ID No photo | 2s |
|  GH | Ghana Drivers License | 4s |
|  GH | Ghana Passport | 1s |
|  NG | Nigeria BVN MFA | 1s |
|  KE | Kenya National ID No photo | 3s |
|  GH | Ghana SSNIT | 1s |
|  KE | Kenya Passport | 2s |
|  KE | Kenya Drivers License | 3s |

Note on chart and data set:

This report uses anonymized data collected from transactions on Smile ID. Data in this chart was collected from January to June 2023.

Inclusion: Closing the gender gap

Inclusion is widely regarded as one of three pillars for building equitable and universal ID systems that ensure no one is left behind. As such, it is critical to examine inclusivity in ID verification systems. Without examining inclusivity, disparities in access and use may continue to go unaddressed, resulting in mass disenfranchisement.

Data from Q3 2021 until now show that there has been a significant increase in gender inclusion.

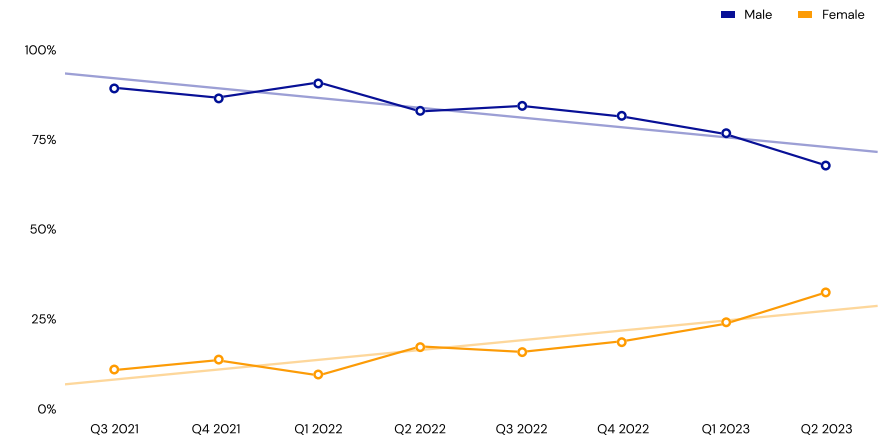
Since the third quarter of 2021, the percentage of female ID verification checks carried out using Smile ID has grown from 10% to 35% in the first half of 2023. This indicates positive progress in addressing gender disparities.

When analysed by industry, BNPL companies have led the way with an average of 30% of verified IDs belonging to female users since 2021.

On the other hand, banking and lending companies have made the most improvements regarding gender inclusion, increasing onboarded female users from 9% to 36%.

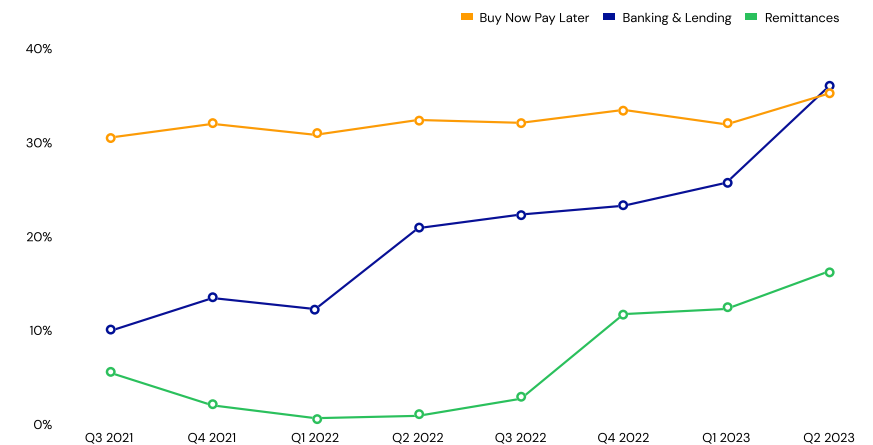
Gender Distribution of Digital Identity Checks by Smile ID

% of KYC checks, by Gender



% Female Digital Identity Checks by Smile ID for Banking, Credit and Financial Inclusion Services

% of KYC checks, by Gender



Note on chart and data set:

This report uses anonymised data collected from transactions on Smile ID. Data in these charts was collected from July 2021 to June 2023.

Fraud: down, but not out

In the first half of 2023, we saw fraudulent onboarding attempts fall across Africa as compared to the previous year. In H1 2023, the total number of **fraudulent KYC attempts** caught by Smile ID decreased by 5 points to **23% from a peak of 28% in 2022**.

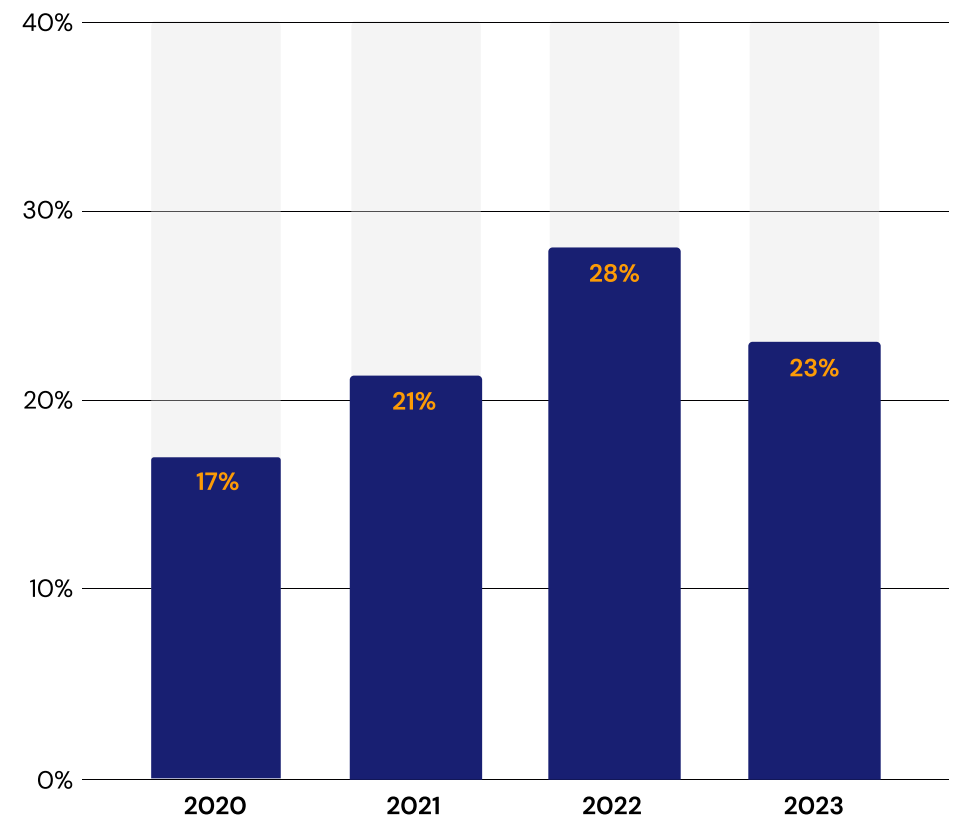
The decline in fraud rates coincides with declining startup funding across the continent. **Venture funding in Africa dipped by over 50%** year-on-year in the first half of 2023. More so, the number of startups that received funding dropped from 303 in H1 2022 to 131 in H1 2023. This decrease in funding has led to reduced marketing spend, especially incentive-based acquisition, which has been shown to have a high correlation with increased fraud attempt rates.

However, with cybercriminals persistently adapting, businesses must stay vigilant in combating fraud. While referral fraud rates have dropped significantly, cybercriminals are still looking to exploit digital platforms to scam other users or funnel illicit earnings. Based on conversations with our clients, we also believe that as digital onboarding formalises, fraudsters are re-focusing their energy on transactions rather than account creation; this reinforces the need for multi-factor authentication, including biometrics.

This report explores the latest identity fraud trends and countermeasures, examining evolving fraudster tactics and the impact of new product initiatives. We aim to empower businesses to protect their customers and contribute to a more secure digital Africa.

Fraudulent attempts caught by Smile ID

% of Total KYC Checks



Note on chart and data set:

This report uses anonymised data collected from transactions on Smile ID. Fraudulent KYC checks include biometric fraud and data validation errors when checking against government ID databases. Data in this chart was collected from 2020 to June 2023.

Verification is critical; collecting documents is not enough

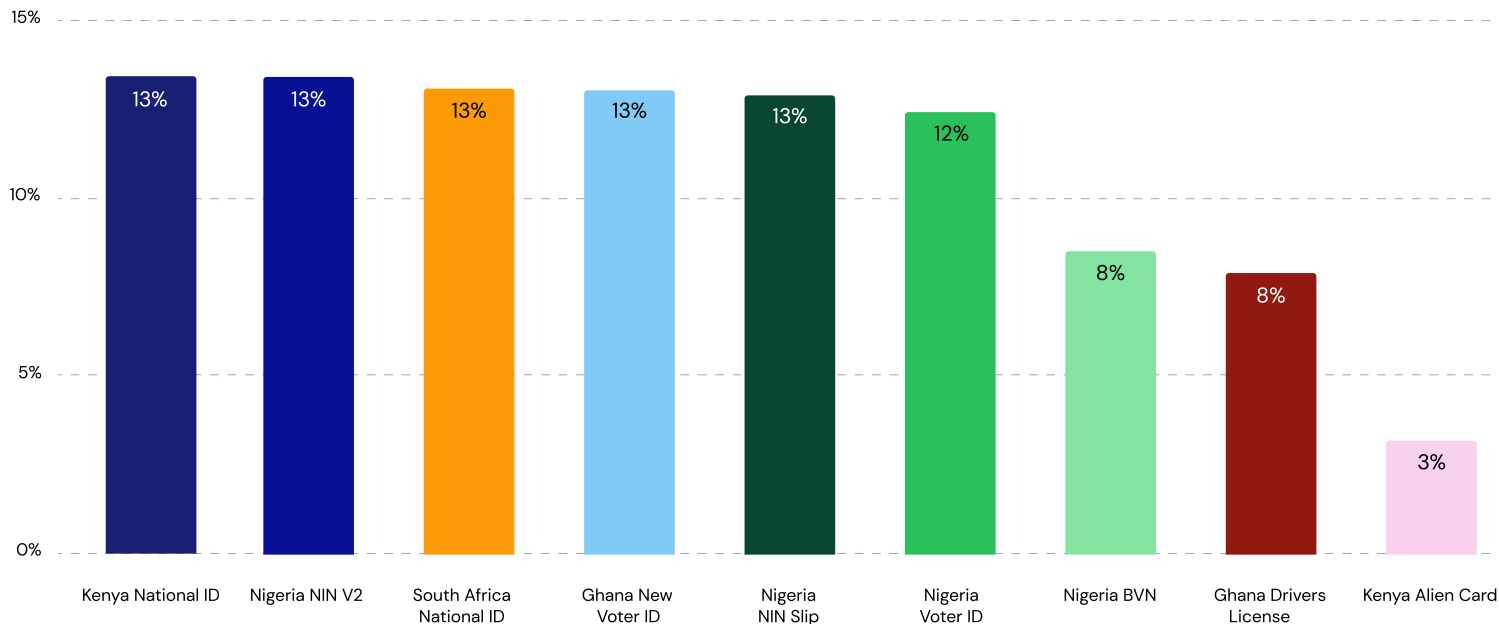
As African countries work to centralise their identity databases, national IDs have become the most ubiquitous form of identity document. They are also used for accessing government services like social welfare programs, paying taxes and acting as foundational documents for obtaining functional IDs like passports or driver's licences.

Scammers frequently attempt to use forged or stolen national IDs to gain fraudulent access to regulated services. The implication of this is that businesses can no longer afford to stop their KYC processes by just collecting documents.

In the first half of 2023, the national IDs of Kenya, Nigeria and South Africa were the three most frequently targeted types of IDs for fraud relative to other forms of identification across Africa. Specifically, in these three countries, national ID cards experienced a higher fraud rate than any other form of ID during the first half of 2023.

Biometric Fraud attempts caught by Smile ID

% of Total KYC Checks, by ID Type



Note on chart and data set:

This report uses anonymized data collected from transactions on Smile ID. Biometric fraud rates are measured by Smile ID between January and June 2023; includes approximately 22 million KYC checks across Africa; selected countries and ID types with significant volumes.

While different ID types may be more vulnerable to particular types of fraud, the majority of ID-related fraud attempts across Africa take one of the following formats:



Selfie Spoofs

where scammers with stolen IDs attempt to pass themselves off as the owners of the documents by using a photo to impersonate someone else. This can include using a picture of a printout, a saved image or video from a device, a printed face mask, or even a lifesize cardboard cutout.



Face Mismatches

where a valid ID number is provided, but facial biometrics do not match the ID.

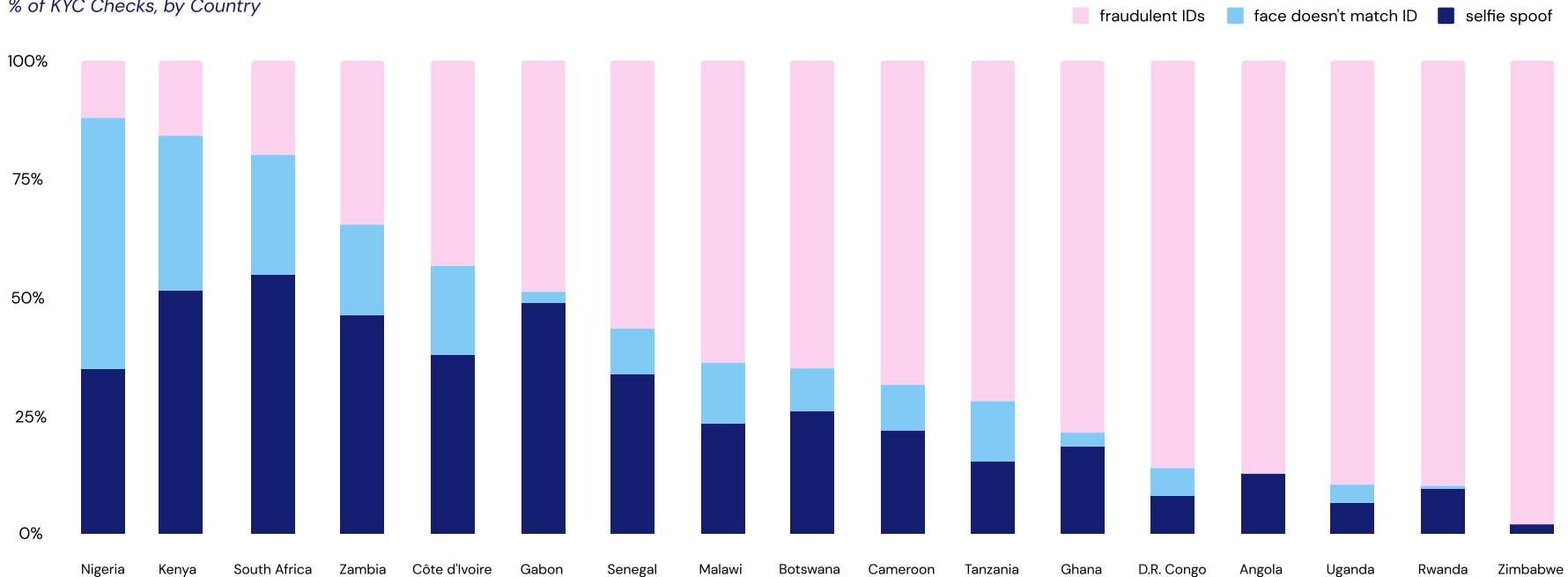


Fraudulent IDs

these could be counterfeit IDs, unacceptable ID types, tampered documents, expired IDs or times when an actual ID card was not provided.

Fraud Types Caught by Smile ID Biometrics

% of KYC Checks, by Country



Note on chart and data set:
This report uses anonymized data collected from transactions on Smile ID. Biometric fraud rates are measured by Smile ID between January and June 2023; includes approximately 22 million KYC checks across Africa; selected countries and ID types with significant volumes.

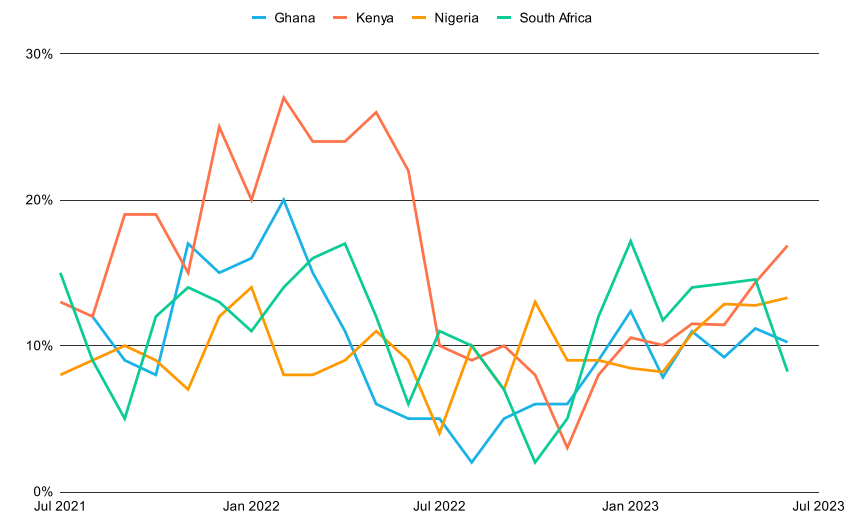
Fraud trends across the four key startup markets

Convolutional Neural Networks, or layers upon layers of coded logic that look for features or patterns, have driven major advances in computer vision in the last five years. These advances have enabled high accuracy even in challenging image conditions such as low-lighting environments or partially obscured images. These technologies have proven particularly beneficial during the onboarding process in African markets, where image quality and capture conditions can vary dramatically.

As more businesses across Africa adopt biometrics for identity verification and fraud prevention, more fraud is being caught, and more valid users who may have previously been rejected due to poor image quality are approved, helping improve onboarding conversion metrics and customer satisfaction.

Biometric Fraud attempts caught by Smile ID

% of Total KYC Checks, by country



Note on chart and data set:

This report uses anonymized data collected from transactions on Smile ID. Biometric fraud rates are measured by Smile ID between July 2021 and June 2023; includes approximately 10 million KYC checks across Africa; selected countries and ID types with significant volumes.

Kenya and South Africa in Focus

After seeing record-low numbers in H2 2022, **fraud in Kenya is rising again**. In the first half of the year, fraud attempts grew from 10% in January 2023 to 17% in June 2023. However, even though there has been a significant increase, fraudulent onboarding attempts are still below the figures recorded in H1 2022. The recent increase in fraud attempts makes Kenya the highest-risk country for ID fraud compared to the other countries analysed – a position it has not held since H1 2022.

After finishing in December 2022 as the country with the highest risk for ID fraud, we have observed a significant drop in ID fraud rates in South Africa. Between January 2023 and June 2023, **fraud rates in South Africa dropped from 17% to 8%**. These figures make South Africa the lowest-ranking country for onboarding fraud and the only country with a single-digit percentage of fraud attempts.

As we continue to monitor these trends, it becomes evident that the battle against biometric fraud is ongoing, requiring constant vigilance and the implementation of innovative strategies to safeguard the security of identity verification systems across these countries. Fraud rates move up and down across countries as growth and user behaviour changes in response to new products, services or changes in regulations.

The biometric KYC solution at Smile ID involves matching a user's submitted selfie with the photo on their government-issued ID documents. This approach combines the reliability of document verification with the added assurance of biometric verification, ensuring that your users are indeed who they claim to be, and has proven to reduce fraudulent users by 50%.



BNPL fraud rates drop significantly; Crypto and Payments on the rise

Identity fraud rates in the BNPL industry have fallen to a record low of 4% from 37% in the previous time frame.

In contrast, Africa's cryptocurrency sector continues to grapple with high fraud rates, while the payments and remittances industries are witnessing a marked increase in fraud from last year.

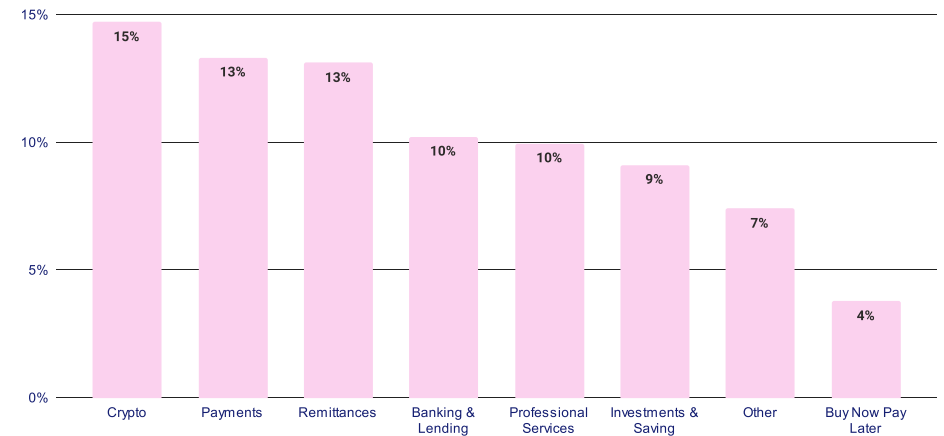
A thorough analysis of fraud across various industries reveals that all sectors experience significant biometric fraud attempts that go unnoticed when using textual checks alone. In particular, the payments sector could greatly benefit from biometric solutions due to its reliance on high volumes of text-only validation, which involves non-biometric jobs where users only submit an ID number for verification against a database.

Relying solely on textual KYC can lead to 50% more undetected fraud, as most fraudsters can only be identified through biometric checks.

By incorporating biometric verification methods, businesses can enhance their security measures, better detect fraudulent activities, and protect their platforms and users. As the payments and remittances industries continue to grow in Africa, integrating biometric solutions will be crucial for maintaining trust and ensuring the safety of transactions within these sectors.

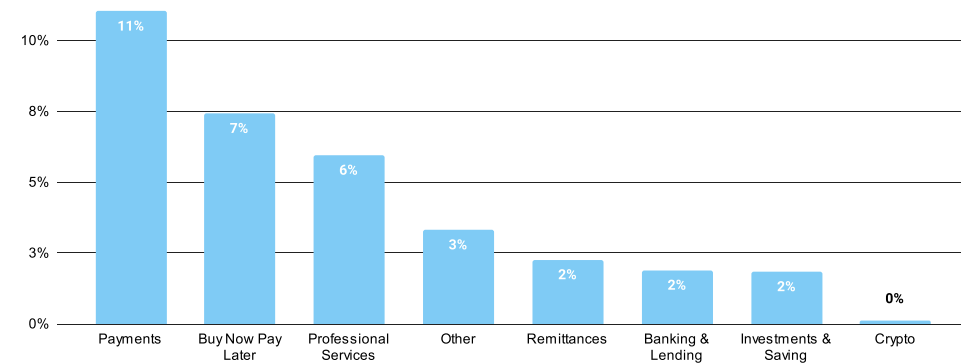
Biometric Fraud Rate by Industry

% of total within industry; Africa average



Data Validation Fraud Rate by Industry

% of total within industry; Africa average



Note on chart and data set:

The biometric and data validation/textual KYC charts reflect different companies based on their usage of Smile ID. As such, not all categories are represented as we exclude certain categories that don't pass a statistically significant threshold in volume. This report uses anonymised data collected from transactions on Smile ID between January and June 2023; includes approximately 22 million KYC checks across Africa; selected countries and ID types with significant volumes.

National ID database uptime is improving in 2023

The first half of 2023 has seen a significant improvement in the uptime of national ID databases across Africa compared to the second half of 2022. In FY2022, the average downtime during a 24 hour period was 6%, with a maximum downtime during a day of 63% and 37 days with 10% or more downtime. However, in H1 2023, the **average downtime has reduced to 3%**, with a maximum downtime of 18% and 19 days with 10% or more downtime.

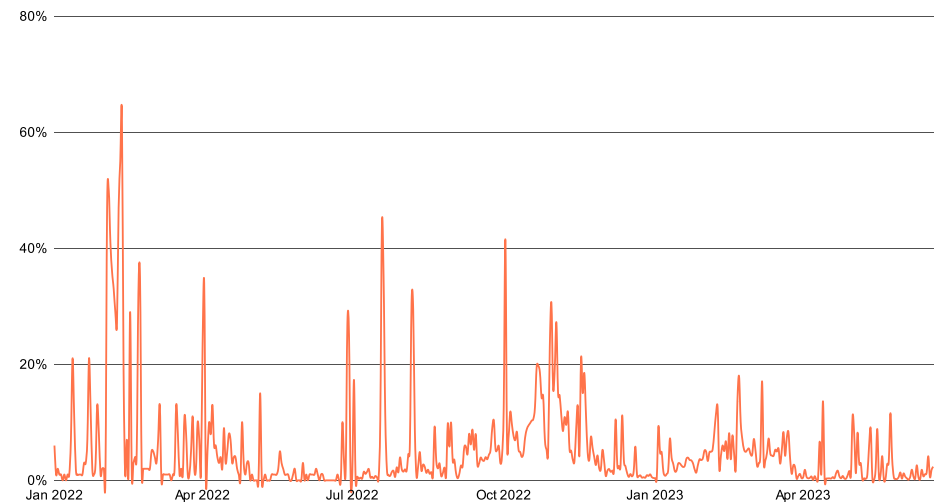
Though there has been a significant improvement, the fact is frequent database downtimes are still a major obstacle to real-time verification, and relying solely on national ID databases can lead to interruptions in business continuity.

To mitigate downtime and provide coverage where reliable national ID databases do not exist, Smile ID offers Document Verification, a comprehensive and global solution for onboarding. Document Verification involves collecting and verifying user-submitted identity documents.

Document Verification is a better, more effective and more reliable way to launch in multiple markets or handle users from different countries with one integration. It serves as the primary source of truth, allowing businesses to combine biometric checks and government checks to enhance their onboarding fraud prevention strategies. With Document Verification, businesses can ensure the integrity of their identity verification systems, even during national database downtimes.

Daily ID Database downtime

Measured as the % of KYC checks by Smile ID that could not be completed; Africa average



| | FY2022 | H1 2023 |
|----------------------------------|--------|---------|
| Average Downtime within 24 hours | 6% | 3% |
| Max Downtime within 24 hours | 63% | 18% |
| Days w/ 10%+ downtime | 37 | 19 |

Note on chart and data set:

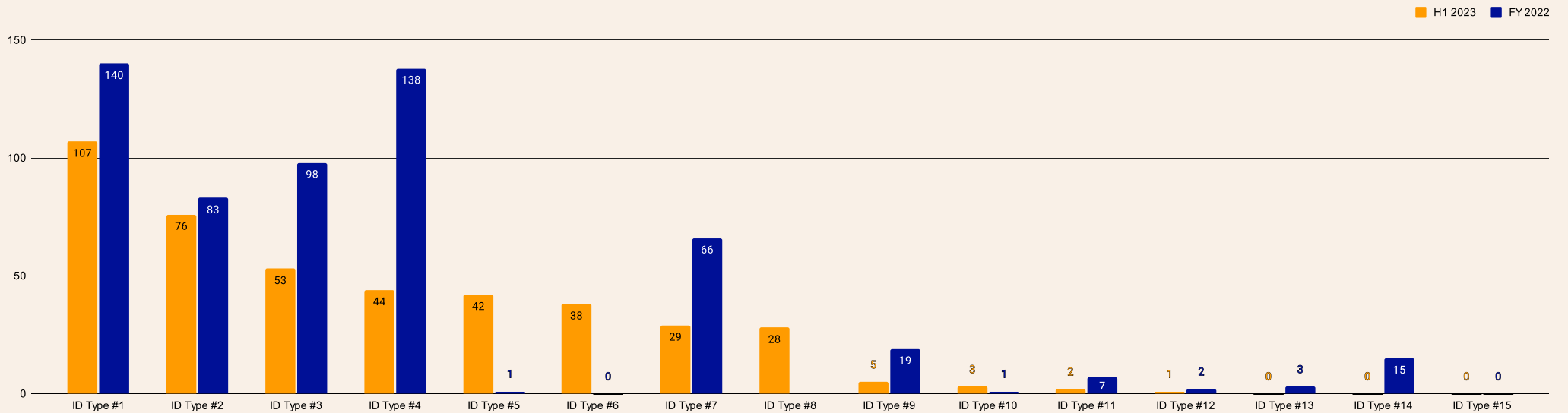
This report uses anonymized data collected from transactions on Smile ID between January and June 2023; includes approximately 22 million KYC checks across Africa; selected countries and ID types with significant volumes.

Some ID types experience more frequent downtimes

Some ID types experience more downtime, leading to service disruptions for users accessing these platforms. Nevertheless, in the past six months, all ID types have improved. The ID type with the most downtime had 107 days, compared to 140 in 2022. Smile ID clients can switch between popular ID types to reduce disruptions for their business and end users.

Days with more than 10% Downtime comparison between Full Year 2022 and H1 2023

During 365 day period from Jan to Dec 2022 and 180 day period from Jan to June 2023; measured by the % of KYC checks that could not be completed



Note on chart and data set:

This report uses anonymized data collected from transactions on Smile ID between January and June 2023; includes approximately 22 million KYC checks across Africa; selected countries and ID types with significant volumes.

Country Deep Dives: KYC Compliance Across Africa



The Big Story: South Africa, Nigeria & Cameroon now on FATF grey list

In the first half of 2023, the Financial Action Task Force (FATF) added South Africa, Nigeria, and Cameroon to its Grey List, bringing the total number of African countries on the list to 11. Other countries on the list include Burkina Faso, the Democratic Republic of Congo, Mali, Mozambique, Senegal, South Sudan, Tanzania, and Uganda.

Greylisting by the FATF implies that a country has been identified as having strategic deficiencies in its anti-money laundering (AML) and counter-terrorism financing (CTF) regimes that they must fix within an agreed timeframe. While on the greylist, businesses and consumers in these countries can be subjected to additional compliance requirements and international trade restrictions. Here's a summary of the FATF's assessment of the three countries.



Nigeria

The FATF's assessment found that Nigeria had made progress in addressing some of the deficiencies but still had work to do in areas such as customer due diligence, suspicious activity reporting, and the regulation of non-profit organisations.



South Africa

The FATF's assessment found that South Africa had a solid legal framework for combating money laundering and terrorist financing but had significant shortcomings in its implementation.



Cameroon

The FATF found that while Cameroon had made some progress in addressing its deficiencies, it had work to do in developing a risk-based AML/CFT framework and investigating and prosecuting offenders.

We expect the recent additions to the FATF grey list to significantly impact the KYC ecosystem on the continent due to the growing number of countries on the list and the profile of countries now involved. Nigeria and South Africa are Africa's two biggest economies representing approximately 30% of the continent's GDP, and regulators and investors apply more scrutiny when dealing with transactions from greylisted countries.

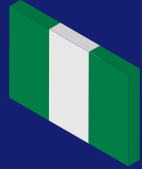
How businesses should respond:

As with all other countries on the greylist, Nigeria, South Africa, and Cameroon have committed to improving their respective AML/CFT regimes, meaning that all three nations can be expected to introduce new regulations for accountable organisations. South Africa leads the way already, announcing amendments to its AML/CFT laws in the first half of the year.

Now more than ever, businesses across Africa must ensure their KYC/AML procedures are on par with international best practices. With the global focus on combating financial crimes intensifying, companies operating in the continent must prioritise robust KYC/AML procedures to safeguard their operations, protect their reputation, and contribute to the overall integrity of the financial system. Companies must also be nimble, staying up-to-date with regulatory developments and engaging in ongoing training and education.



Nigeria



KYC Verification Requirements:

Name, Date of Birth, ID Document

Acceptable ID Documents:

NIN, National ID Card, BVN, Driver's License, Passport, Voters ID

KYC Data Storage Period:

10 years

Data Compliance Regulation:

[National Data Protection Bill](#)



Population
222.4 Million



Population with ID
85%



Median Age
18



Primary ID Issuer
National Identity Management
Commission (NIMC)

Population with ID represents people 15 years+

The National Identification Number (NIN) issued by the National Identity Management Commission is the foundational ID document for identity verification in Nigeria. It has the widest coverage of any ID document, with over 100 million enrollees. Functional IDs used for identity verification in Nigeria include the Voter's ID card, International Passport, Driver's License and BVN.

NIN enrollment crosses 100 million registration benchmark

By the end of May 2023, Nigeria's National Identity Management Commission (NIMC) crossed the 100 million benchmark for the number of unique registrations. This achievement solidifies NIN's standing as the most widely-held identity document in the country.

In recent months, the NIMC has scaled its infrastructure to enroll more Nigerians into its database by working with telecoms, agent networks and other institutions to increase registrations and awareness.

The benchmark brings Nigeria closer to the World Bank's recommendation of enrolling 148 million by June 2024, a goal that authorities are confident about meeting.

Source: [National Identity Management Commission](#)

New policy empowers banks to issue debit cards as ID documents

To increase access to physical versions of the national ID card, Nigeria's Federal Executive Council has approved a policy allowing commercial banks to issue debit cards that double as identity documents.

Over the last few years, the Nigerian government has sought to increase the coverage of its identity database by making National Identity Number (NIN) enrollment mandatory for bank account ownership and sim card usage. While enrollment efforts have been successful, access to physical documents is still low.

Legally, the NIN is the only requirement for identifying Nigerian citizens and residents, and it is typically issued a few weeks after enrollment. The National Identity Management Commission (NIMC) also launched a mobile app in 2021 that allows users access to an e-ID. However, demand for physical cards remains high, especially in rural regions where many people don't have access to the NIMC app.

Following the recent announcement, banks will be able to print multipurpose debit and credit cards that double as physical versions of the holder's national ID card at no extra cost. This move is expected to increase access to physical ID documents for users in both urban and rural regions.



South Africa



KYC Verification Requirements:

Name, Date of Birth, Phone Number, ID Document

Acceptable ID Documents:

Smart ID Card, Green Card, Driver's License, Passport

KYC Data Storage Period:

10 years

Data Compliance Regulation:

Protection of Personal Information Act (POPIA)



Population
60.8 million



Population with ID
92%



Median Age
27.1



Primary ID Issuer
Department of Home Affairs

Population with ID represents people 15 years+

The Smart ID card issued by the South African Department of Home Affairs is the foundational ID document for identity verification in the country. It was introduced in 2013 to replace the older Green Booklet. Functional IDs like a passport, driver's licenses, and resident cards can also be used to verify identities.

Identification Bill Proposes an Integrated Biometric System for South African Residents

In February 2023, South Africa's Ministry of Home Affairs announced a new National Identification and Registration bill that aims to introduce a single, integrated biometric national identification system for all persons living in South Africa.

Currently, South Africa has three independent databases for people: the national population register, the biometric national identity system and the visa adjudication system. The newly proposed integrated database will homogenise all three databases and contain the identity information of everyone resident in South Africa, including citizens, legal residents and visitors.

In addition to the integrated database, the new bill proposes reducing the legal age for obtaining a national ID card from 16 to 10 years.

Kenya



KYC Verification Requirements:

Name, Address, ID Document

Acceptable ID Documents:

National ID Card, Driver's License, Passport, Alien Card, Resident Card

KYC Data Storage Period:

7 years

Data Compliance Regulation:

[Kenyan Data Protection Act](#)



Population

57.5 million



Population with ID

91%



Median Age

19



Primary ID Issuer

**Integrated Population
Registration System**

Population with ID represents people 15 years+

The Kenyan National Registration Bureau issues the National ID card as the foundational ID for identity verification in the country. Functional IDs like driver's licenses, international passports, alien cards, and refugee IDs can also be used to verify identities.

Kenya's new digital identity is equipped with biometric features

More information has been unveiled about Kenya's soon-to-be-implemented digital ID system. The new ID system, known as Unique Personal Identifiers (UPI), is earmarked for roll out in September 2023.

In May 2023, the Kenyan government announced that it would be equipping the digital id with enhanced security features such as iris and facial biometrics and the fingerprint identification system used in current identity documents.

The new ID system is expected to create enhanced possibilities for online ID authentication and give Kenyans more control over sharing their personal data.

Ghana



KYC Verification Requirements:

Name, Date of Birth, Place of Birth, ID Document

Acceptable ID Documents:

Smart Card, Voter's ID, Driver's License, SSNIT, Passport, Resident Card

KYC Data Storage Period:

6 years

Data Compliance Regulation:

[Ghana Data Protection Act](#)



Population

33 million



Population with ID

84%



Median Age

20



Primary ID Issuer

National Identification Authority

Population with ID represents people 15 years+

The National Identification Authority issues the Smart Card as the foundational ID document for identifying citizens and legal residents in Ghana. Functional IDs like an International Passport, Voters ID, Social Security and National Insurance Trust (SSNIT), and resident card can also be used to verify identities.

17.4 million Ghanaians enrolled on the Ghana Card

Speaking at the 2023 ID4Africa meeting in Nairobi, Prof. Kenneth Attafuaah, the Executive Secretary of Ghana's National Identification Authority (NIA), announced that the country's biometric card initiative had registered over 17.4 million holders by April 2023.

This achievement represents an over 280% increase from 2017 when the initiative had only registered 4.5 million Ghanaians. The agency also stated that 17.2 million cards had been printed for registered holders, and 16.2 million had been collected.

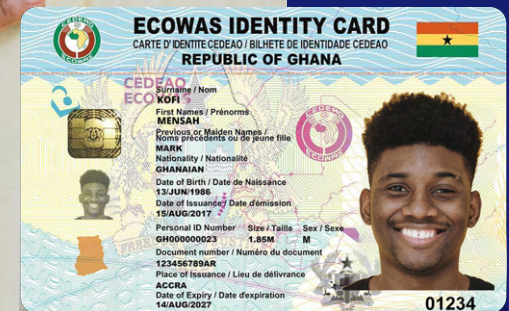
Source: [ID4Africa](#)

Ghana Drops Age Requirement for Ghana Cards

Ghana has dropped the age of its Ghana Card registration to include newborns. This development comes as part of Ghana's plan to evolve its national identification system to be on par with developed countries around the world.

In earlier years, the Ghanaian government has sought to standardise the Ghana Card as the primary identity document in the country, merging it with the Social Security and National Insurance Trust, National Health Insurance Scheme and Tax Identification Number, among others.

The new policy sees the Ghana Card complete its transition from an identity document to a lifelong identifier for all Ghanaian citizens. While children will now be registered for their Ghana Card number, it is unclear whether they or their guardians can apply to get the physical card until they reach the age of 15.



Uganda



KYC Verification Requirements:

Name, Address, ID Document

Acceptable ID Documents:

National ID, Voter's ID, Driver's License, Passport

KYC Data Storage Period:

10 years

Data Compliance Regulation:

[Data Protection and Privacy Act of 2019](#)



Population
50.4 million



Population with ID
70%



Median Age
16



Primary ID Issuer
National Identification and
Registration Authority of Uganda

Population with ID represents people 15 years+

Uganda's National Identification & Registration Authority (NIRA) issues the National ID card as the foundational ID for identity verification. Functional IDs like a passport, voter IDs and driver's licences can also be used to verify identities.

Uganda's NIRA issues over 26 million NINs

The National Identification and Registration Authority of Uganda (NIRA) announced in May 2023 that it has issued citizens over 26 million National Identification Numbers (NINs). This brings NIN coverage in Uganda to over 95% of the adult population — a feat achieved within nine years of the commencement of the ID program.

Despite having extensive NIN coverage, many Ugandans still lack physical ID documents. In its statement, NIRA announced that it had printed over 19 million National ID cards, but only 16 million have been collected, leaving the agency with over 3 million uncollected cards. The agency has urged registered Ugandans to collect their cards before transitioning to a digital ID system.

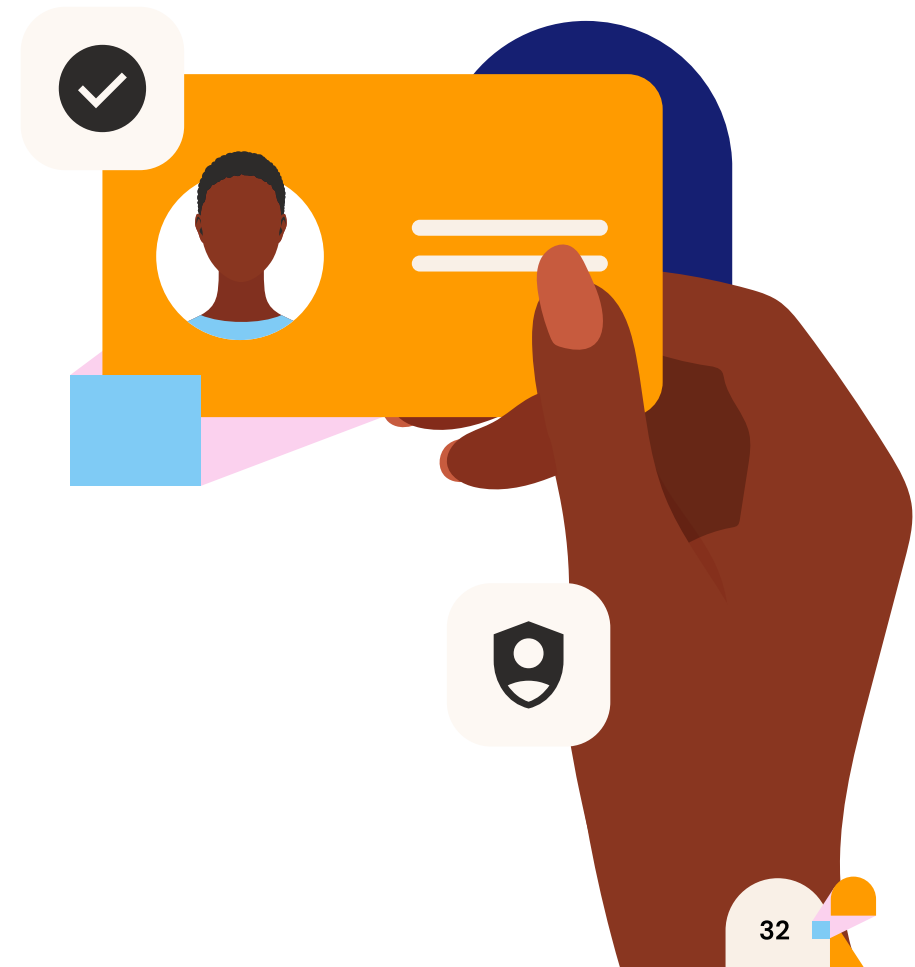
Source: [New Vision](#)

Uganda's Digital ID Transition Faces Challenges

In April 2023, the Auditor General of Uganda, John Muwanga, raised concerns about the country's lack of preparation for transitioning to the new digital ID cards. In 2022, Uganda announced a transition to a new generation of digital ID cards implanted with microchips containing citizens' electronic and biometric information.

While the transition is expected to commence in 2024, the Auditor General expressed doubts about NIRA's ability to handle the transition smoothly, citing a lack of adequate preparation and strategising ahead of the commencement date.

In a follow-up statement, NIRA reiterated that they were still within time to prepare for the ID roll out and were in the advanced planning stages.



Rwanda



KYC Verification Requirements:

Name, Date of Birth, Passport Photograph, ID Document

Acceptable ID Documents:

National ID, Driver's License, Passport, Refugee Card, Non-citizen ID

KYC Data Storage Period:

6 years

Data Compliance Regulation:

[Data Protection Law](#)



Population
13.9 million



Population with ID
90%



Median Age
20



Primary ID Issuer
National Identification Agency

Population with ID represents people 15 years+

Indangamuntu, or the Rwandan national ID, is the foundational ID document issued by the National Identification Agency of Rwanda. Functional documents such as driver's license, international passport, refugee ID, and non-citizen ID can also verify identities.

Rwanda to Expand Digital ID Access to Stateless Persons and Children

The Rwandan parliament has commenced the process of creating a more inclusive ID system that captures children and stateless persons resident in the country.

The recently proposed amendment to the country's law on the registration of persons and issuance of the national ID card allows for the creation of the Rwanda Single Digital System (SDID), which the country expects to close gaps in its existing ID architecture.

The new scheme, which the World Bank funds, is expected to be executed within a 3-year period from when the legislative framework is put in place.

Source: [KTPress](#)

Tanzania

KYC Verification Requirements:

Name, Date of Birth, Place of Birth, Address, ID Document

Acceptable ID Documents:

National ID, Voter's ID, Passport, Driver's License, Health Insurance ID, Refugee ID, Resident ID

KYC Data Storage Period:

10 years

Data Compliance Regulation:

Personal Data Protection Act (PDPA)



Population

65.2 million



Population with ID

~90%



Median Age

18



Primary ID Issuer

National Identification Agency

Population with ID represents people 15 years+

Tanzania's National Identification Authority (NIDA) issues the National Identity Card, the foundational ID for identity verification. Voter IDs, driving licenses and international passports are functional ID documents that can be used to verify the holder's identity.

Tanzania deactivates 970,000 unverified sim cards

The Tanzanian government deactivated 970,000 unverified sim cards to reduce fraudulent activities in February. The deactivation resulted from non-compliance with the Tanzania Communications Regulatory Agency's (TCRA) 2019 directive for all citizens to register their sim cards biometrically.

The sim registration services required telcos to run biometric checks against their national ID cards on mobile phone users. Although the exercise was initially scheduled to end on January 31st, the TCRA extended it to February 14 to allow more people to register.

Despite the deactivation of nearly a million sim cards, the registration exercise has been largely regarded as a success, as 60.47 million of 62 million mobile users in the country registered before the policy deadline. The exercise has also been linked to a rapid drop in cases of sim card fraud.

Source: *Developing Telecoms*

Ethiopia



KYC Verification Requirements:

Name, Place of Birth, Date of Birth, Address, ID Document.

Acceptable ID Documents:

Fayda ID, Kebele ID, Driver's License, Passport, Resident Card, Non-citizen ID

KYC Data Storage Period:

N/A

Data Compliance Regulation:

Data Protection Proclamation (Still in Progress)



Population

108 million



Population with ID

92.2%



Median Age

24



Primary ID Issuer

Civil Status Department
(Ministry of Interior)

Population with ID represents people 15 years+

The National Identity Program (NDIP), in 2022, started enrollment for the Fayda ID, which serves as Ethiopia's foundational ID document for identity verification. Currently, the NDIP has enrolled just over 1.4 million Ethiopians for the Fayda ID.

The Kebele ID, which is used to identify a person's ward or residence is currently the most popular ID type, with ID4D placing popularity between 90 - 95% among adults. The Kebele ID and other functional IDs like driver's licenses, international passports, non-citizen IDs, and resident cards can verify the holder's identity.

Ethiopia Passes Digital ID Law

In March 2023, Ethiopian lawmakers announced the approval of the country's Digital Identity Proclamation bill into law. This bill makes Ethiopia the latest in a growing list of African countries migrating to a digital ID system.

Ethiopia's digital ID bill is expected to help the country establish a comprehensive, consistent and reliable system for the registration of citizens. The bill covers various issues, including registration, authentication services, the institutional framework, data security, privacy protection, and criminal liability.

It has been hailed as an important step in modernising the country's ID system and is expected to have multiple benefits, including improving national development and enhancing inclusiveness.

Source: [Addis Standard](#)

Fayda ID to become mandatory for financial transactions

The National Bank of Ethiopia, and the National Identity Program in July, made a joint statement announcing plans to make the country's national digital ID, Fayda, mandatory for all transactions. According to a 2017 report, 34.83% of Ethiopia's adult population (~23.7 million people) had bank accounts.

Per early statements, the initiative will mandate bank customers to use the Fayda ID as their bank ID for KYC checks and completing remote onboarding. This joint initiative is expected to help the country achieve its goal of 45 million enrollments in 2024 by making more people enroll for the Fayda ID. The National Bank of Ethiopia, which is the country's central bank has also assured that the plan to use the Fayda as primary ID for banking operations will significantly improve transparency, stability and security in Ethiopia's financial sector.



Egypt



KYC Verification Requirements:

Name, Address, ID Document

Acceptable ID Documents:

National ID, Passport, Driver's License, Resident ID

KYC Data Storage Period:

5 years

Data Compliance Regulation:

[Personal Data Protection Law](#)



Population

108 million



Population with ID

92.2%



Median Age

24



Primary ID Issuer

Civil Status Department
(Ministry of Interior)

Population with ID represents people 15 years+

The Egyptian Civil Status Department issues a National ID card as the foundational ID document for all residents and citizens. As of 2021, ID ownership was around 93% of the country's adult population. Driver Licenses, passports and resident cards are functional IDs that can be used to verify identities.

Egypt to Implement 5-Year Tax Exemption for Startups

In line with its goals of encouraging technological innovation, the Egyptian government has declared a 5-year tax exemption for startups in the country.

Over the last five years, Egypt has become Africa's third most popular destination for startup investment, attracting over \$1.5 billion. The success rate of Egyptian startups with fundraising and building technology solutions has seen the country emerge as the flag bearer for innovation in North Africa.

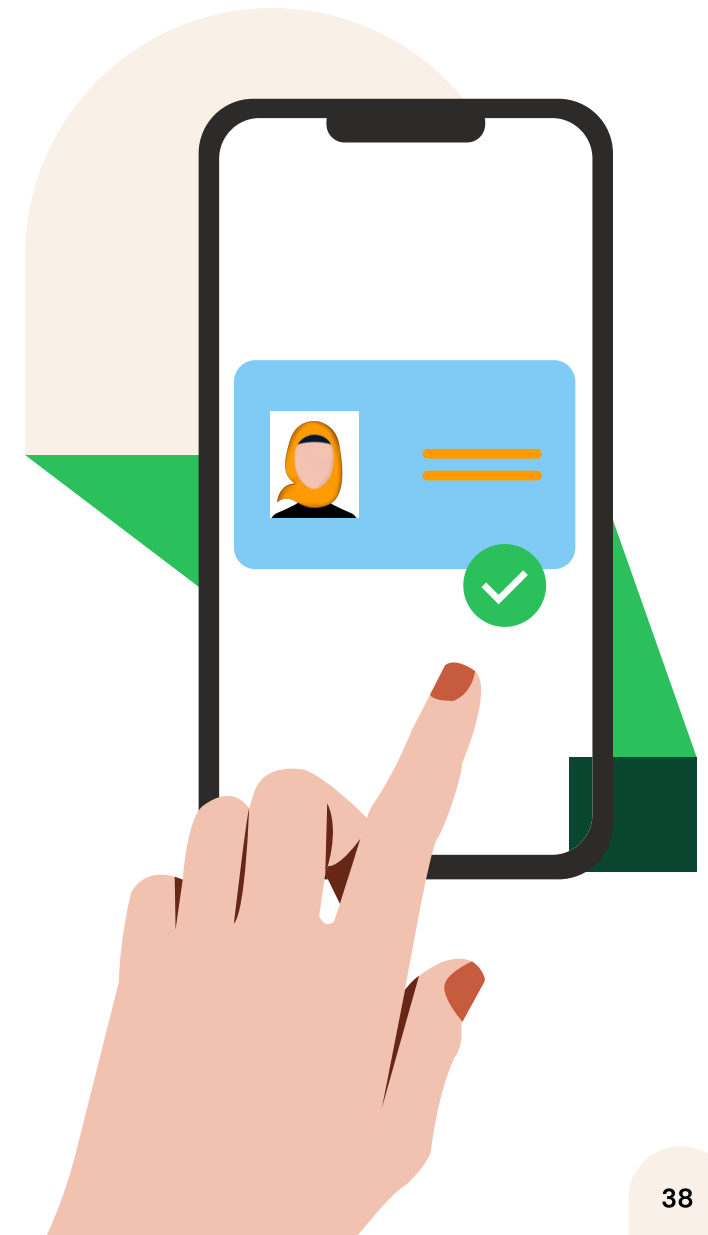
The exemption will be made via legislative amendments to the existing Small and Medium Enterprises Law (Law №152 of 2020), which will be presented to the parliament for approval in the coming weeks.

Egyptian Financial Regulatory Authority Issues New Regulation for the Use of Digital Identity by Non-Banking Entities

The Egyptian Financial Regulatory Authority (FRA) issued new regulations on Wednesday, 12 July 2023, authorising the use of fin-techs and outsources services by non-banking financial services. The Regulation provides a framework for issuing and authenticating digital identity, identity documents, and biometrics in the non-banking financial sector.

The regulation empowers companies licensed as non-banking financial services to provide identity verification and related services. The regulation, however, requires strict compliance with technology infrastructure, information systems, and after-risk recovery and resiliency standards stipulated in the Regulation.

Furthermore, the Regulation requires all service providers of the non-banking services to be registered. Providers must also become joint stock companies within a defined period and secure an insurance policy against technological and professional liability.



Zambia



KYC Verification Requirements:

Name, Address, ID

Acceptable ID Documents:

National ID, Voter's ID, Driver's License, Passport, Registration Card

KYC Data Storage Period:

10 years

Data Compliance Regulation:

[Zambian Data Protection Act](#)

The National ID card issued by the Department of National Registration, Passport, and Citizenship (DNRPC) is Zambia's foundational ID for identity verification. Functional IDs like voter cards, driver's licenses and passports can also be used to verify identities.



Population

20 million



Population with ID

80%



Median Age

16.8



Primary ID Issuer

Department of National Registration, Passport, and Citizenship (DNRPC)

Senegal



KYC Verification Requirements:

Name, Date of Birth, Passport Photograph, ID Document

Acceptable ID Documents:

National ID, Voter's ID, Driver's License, Passport, Ecowas ID

KYC Data Storage Period:

10 years

Data Compliance Regulation:

Act Concerning Personal Data Protection (CPDP)

The national ID card issued by the Agence Nationale de la Statistique et de la Démographie (ANSD) is the foundational ID for identity verification in Senegal. Voter IDs, passports, driver's licenses and the Ecowas ID can also be used to verify the identity of a legal resident or citizen.



Population

18.1 million



Population with ID

72%



Median Age

18



Primary ID Issuer

(Agence Nationale de la Statistique et de la Démographie, ANSD)

Cameroon



KYC Verification Requirements:

Name, Address, ID Document

Acceptable ID Documents:

National ID, Voter's ID, Driver's License, Passport, Resident Card

KYC Data Storage Period:

N/A

Data Compliance Regulation:

N/A (Privacy Bill in the works)

National ID cards issued by the Cameroonian Ministry of Territorial Administration are the foundational ID for identity verification in Cameroon. Voter IDs, driver's licenses, passports, and resident cards can also be used to verify the identities of citizens and residents.



Population
28.5 million



Population with ID
76%



Median Age
17.4



Primary ID Issuer
General Delegation
for National Security

Côte D'Ivoire



KYC Verification Requirements:

Name, Address, ID Document

Acceptable ID Documents:

National ID Card, Driver's License, Passport, Health Insurance Card, Attestation Card, Resident Card

KYC Data Storage Period:

10 years

Data Compliance Regulation:

Protection of Personal Data Law of 2013



Population

108 million



Population with ID

92.2%



Median Age

24



Primary ID Issuer

Civil Status Department
(Ministry of Interior)

Population with ID represents people 15 years+

The Office National de l'État Civil et de l'Identification (ONECI) issues national ID cards that serve as the foundational ID document for identity verification in Côte d'Ivoire. Passports, driver's licenses, resident cards and health insurance identity cards are functional documents that can also be used to verify identities in the country.

Côte D'Ivoire considers Startup Act

As part of its commitment to fostering innovation and entrepreneurship, the government of Côte D'Ivoire has announced plans to launch a Startup Act in the near future. While the exact date of the launch is unknown due to the act still being considered by the country's parliament, government officials insist it is driven by a strong political will to create an enabling ecosystem for Ivorian startups.

The startup act is expected to provide state-of-the-art infrastructure and other amenities to help them succeed regionally and internationally.

In addition to the startup act, the government has put in place plans for technology parks and start-up campuses that it hopes will help the country become a hub for innovation and entrepreneurship.

Source: [TechCabal](#)

Africa's Digital ID transition: Countries to watch

As African countries strive to bring their identity systems up to date, many are turning to digitised systems to create a scalable process. Over the last few years, many African countries have committed to digitising their ID systems in partnership with the world bank's Identification for Development (ID4D) initiative.

The digitisation of ID systems has many advantages, including streamlined administrative processes, better personal data security, improved accuracy, data-driven decision-making, and increased efficiency of identity verification processes. It also indicates a growing market for digital identity verification. Here is a list of countries that have recently made strides in their transition to digital-first ID systems:

Burkina Faso

The West African country has partnered with (Modular Open Source Identification Platform) MOSIP to pilot a national digital ID system. The pilot aims to complete 1000 enrollments; learnings from it will inform a national scale-up program to be designed in the future.

Source: [MOSIP](#)

Kenya

Kenya has announced plans to roll out the Unique Personal Identifier (UPI), a national digital ID system, and foundational document to serve as the primary identity document for Kenyans. It will replace the Huduma Namba which was introduced in 2019 but faced legal challenges to the enrollment procedures and data collection.

Source: [TechCabal](#)

Ethiopia

Following a successful 2022 pilot, Africa's second-largest country by population has off digital enrollment for its foundational Fayda ID document for all citizens and residents with a goal of 45 million enrollees by the end of 2024.

Source: [Biometricupdate](#)

Madagascar

Madagascar's government has entered a memorandum of understanding with MOSIP to execute a pilot of a new national digital ID system. The pilot is expected to enrol 1000 people and provide learnings for future nationwide implementation

Source: [Biometricupdate](#)

Gabon

Reports indicate that Gabon is launching a digital national ID system in December 2023, 10 years after ID cards were last issued in the country. The announcement was made by the country's council of ministers who also announced an extension of the validity of existing ID cards.

Source: [Biometricupdate](#)

Togo

The Togolese Agency for Identification, ANID-TOGO, has partnered with Atos and IDEMIA to build a national biometric eID system. The biometric ID system is expected to be built based on iris, face, and fingerprint recognition technology.

Source: [Atos](#)

Fraud Trends Across Africa



The Big Story: Generative AI and Fraud

Since the second half of 2022, Generative AI has dominated conversations because of its potential impact on increased efficiency, customer experience, and reduced costs due to automation. AI tools like ChatGPT, Dall-E, and Midjourney, among others, have also soared in popularity among everyday tech users, who use them to achieve tasks like research, content creation, image generation, task automation, and more with increasing efficiency.

However, alongside the excitement, there are growing concerns among stakeholders in KYC/AML and fraud-prevention communities about the potential use of AI for malicious purposes, i.e., fraud. Advancements in AI technology mean that fraudsters can create highly realistic versions of forged documents and make more sophisticated attempts at impersonating real people.

Deepfakes are a highly sophisticated form of synthetic computer vision fraud where an existing image or video is replaced with someone else's likeness. These images can make it seem like the target did or said something they did not. Accomplished by superimposing facial images of real people onto videos or 3D computer vision models, deep fakes pose a significant challenge to the integrity of digital media.

Similarly, text-to-image algorithms, or Generative Adversarial Networks (GANs), are computer vision technology that can generate realistic images from textual descriptions. Fraudsters can use these algorithms in identity fraud by creating synthetic images of individuals that do not exist.

While we have yet to detect notable instances or patterns of AI-powered fraud in Africa, we advise businesses to take caution and tighten up loopholes in onboarding processes including using biometrics backed by government databases where possible. In the coming months, companies can expect to see more sophisticated attacks where attackers use deep fakes or GANs to try and game systems. In addition, an increased frequency of attacks should also be expected as AI accessibility is likely to drop associated costs with fake ID creation.

Now, more than ever, it is essential for businesses to engage KYC partners that stay on top of industry trends and are continuously innovating to stay ahead of the market. By doing so, they can better safeguard their systems against the potential misuse of AI and protect themselves and their customers from the risks associated with fraudulent activities.



Common Types of Fraud Attacks

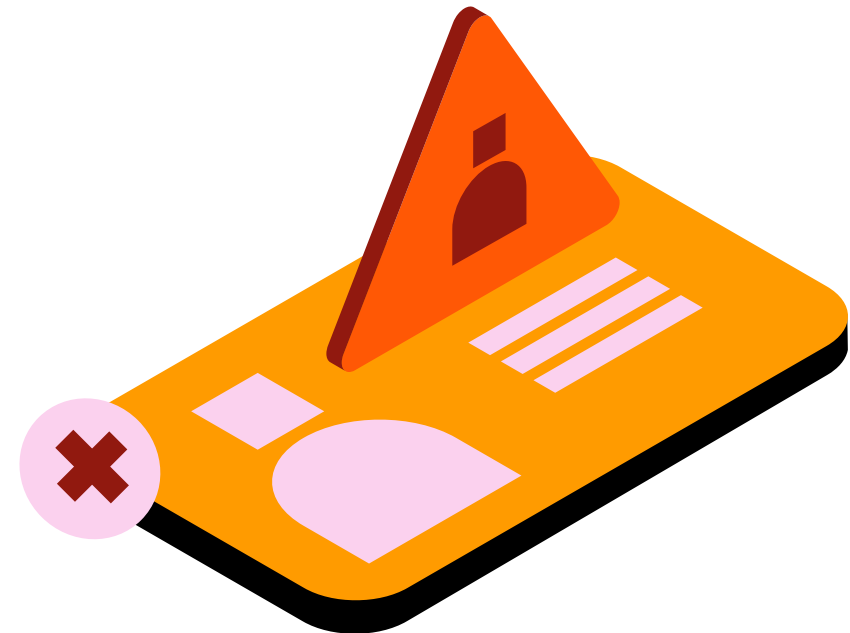
Every day, we help companies across Africa prevent fraud by catching fraudulent users during onboarding. As preventive technology advances, so do the techniques that fraudsters deploy. Here are some fraud tactics we've seen over the last six months.

01. Fake ID documents

Fraudsters commonly use fake or forged ID documents to game a product's onboarding system. Using forged ID documents, fraudsters can create accounts under fictitious identities, facilitating the theft of ill-gotten gains. Depending on how skilled the fraudster is, forged documents can closely resemble the original, allowing them to bypass basic evaluations and eye tests.

Our Document Verification™ product effectively detects such fake IDs by comparing the submitted documents to their authentic templates. This process scrutinises intricate details such as fonts, spacing, holograms, microtext, QR codes, barcodes and watermarks that are challenging to imitate, ensuring fraudulent users are identified and stopped.

In H1 2023, 8% of the documents submitted to Smile ID failed these security feature checks.



02. Stolen ID information

At Smile ID, we find that the majority of fraud attempts involve the use of stolen IDs. This transpires when an individual attempts to register for a service using a document or ID number that belongs to someone else. As these IDs are genuine, a basic KYC check (focusing solely on textual validation) might mistakenly approve them.

Our Biometric KYC solution effectively counters such attacks by comparing user-submitted selfies to official ID photos or documents, swiftly identifying and blocking discrepancies. This process ensures that the person interacting with the service is the legitimate ID holder. This critical component of identity verification extends beyond merely validating the legitimacy and authenticity of an ID or document.

Of all the biometric fraud attempts Smile ID caught in H1 2023, 43% were cases where an ID was valid, but the selfie provided did not match the ID owner.



03. Selfie “Spoofs”

More sophisticated scammers with stolen IDs attempt to pass themselves off as the owners of the documents. One way they do that is through a "selfie spoof," where a person uses a photo to impersonate someone else. This can include using a picture of a printout, a saved image or video from a device, a printed face mask, or even a life-size cardboard cut-out. These spoofs are commonly referred to as "cheap fakes." While similar behaviour may result from genuine user error, such as not following instructions or not understanding the process, spoofs often indicate a fraudster's attempt to impersonate another person.

Our liveness checks ensure that the selfie submitted is a live image of the individual and not a pre-recorded video or photograph.

Selfie spoofs made up 41% of biometric fraud caught by Smile ID in the first 6 months of 2023



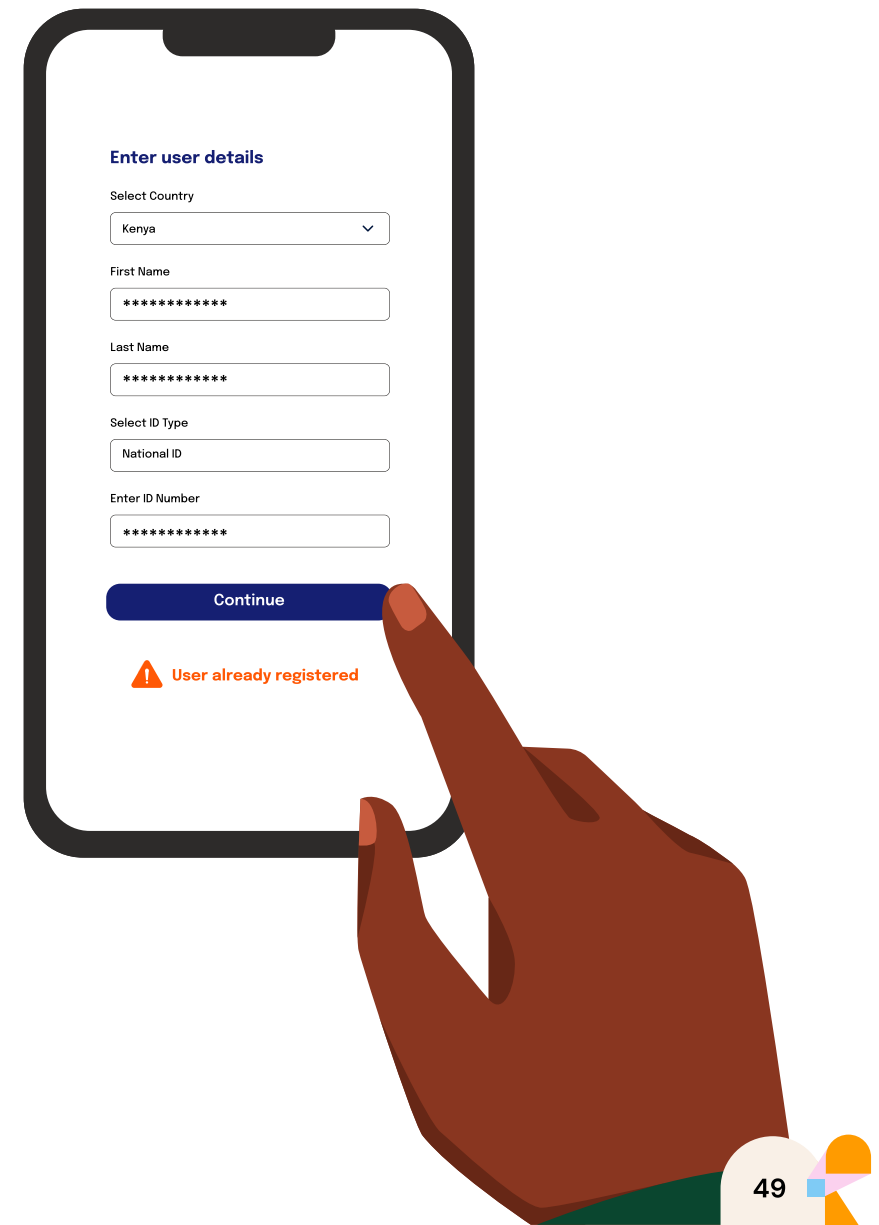
04. Duplication Fraud

This type of fraud occurs when individuals create multiple accounts with a single service provider to exploit reward systems. Such schemes are particularly prevalent among companies that implement promotional incentives—such as referral bonuses or sign-up rewards—to drive rapid growth. The primary aim of such fraudsters is to get away with multiple rewards by creating multiple accounts.

There are two main types of fraudsters involved in this activity. The first type is "Serial Submitters," who repeatedly submit the same ID information or multiple valid IDs of themselves to gain access. While this type of fraud can be pervasive, its success largely hinges on the fraudster's resilience. It can be mitigated by implementing sign-up limits or checks against previously used ID numbers.

The second type of fraudster is known as a "Database Infiltrator." These highly sophisticated fraudsters have unauthorised access to ID authority databases, allowing them to create multiple seemingly legitimate identities. This type of fraud poses a greater risk to any system as their documents will appear valid even during biometric government database or liveness checks. The only way to detect this type of fraud is through biometric de-duplication. At Smile ID, we have seen a user attempt to sign up nearly 300 times with multiple valid IDs. Our biometric de-duplication product Smile Secure was able to identify and surface these repeat attempts.

Learn more on page 60.

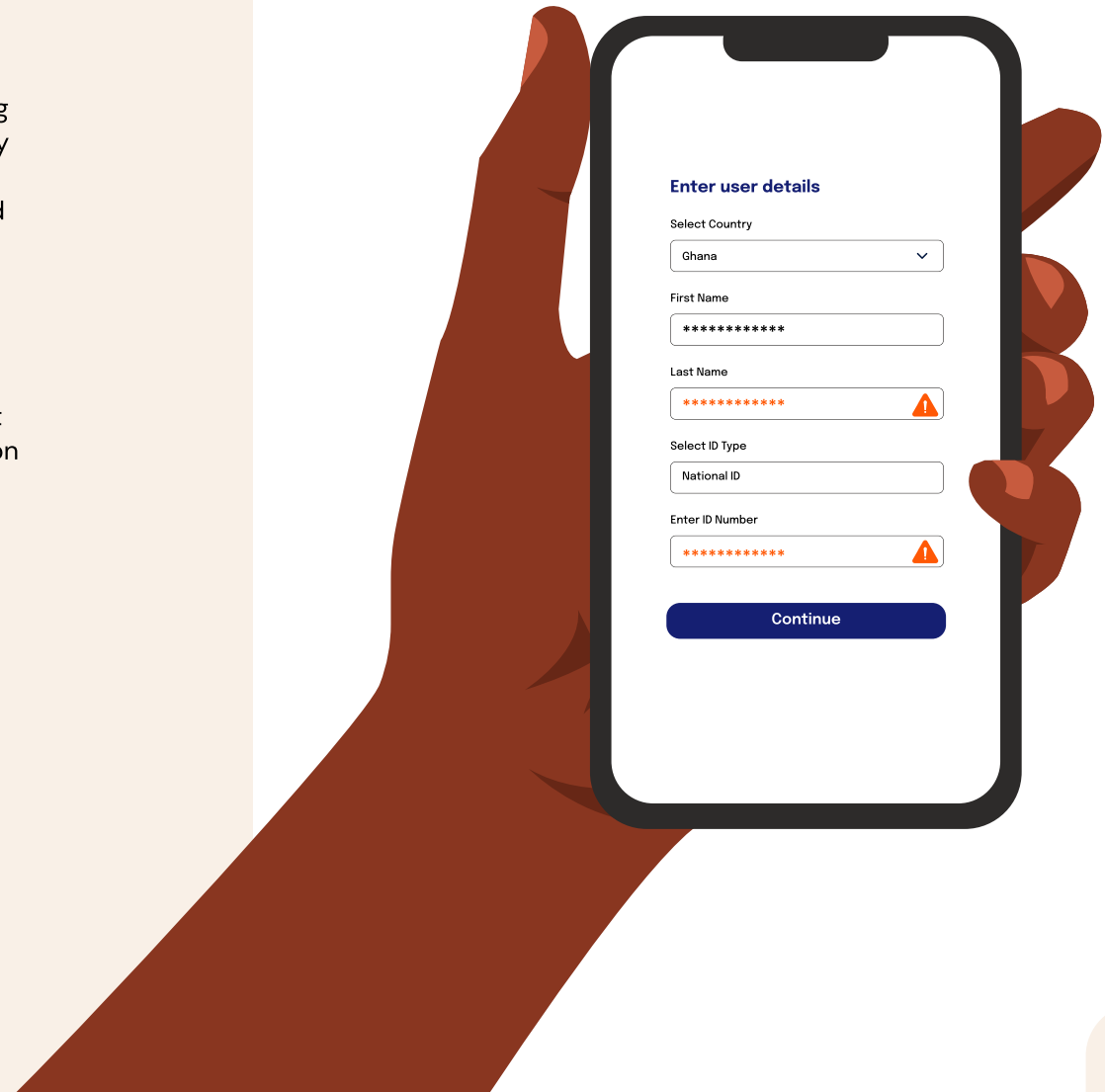


05. Synthetic Fraud

This happens when fraudsters create a new identity by combining real (usually stolen) and fake information. Synthetic fraud is usually more difficult to catch, especially when using only textual verification, as scammers can add a stolen ID number to a falsified document template to fool KYC systems.

While synthetic fraud attempts have typically been low across Africa, recent advancements in AI technology make it a real threat to businesses. Using AI image and video generators, scammers may be able to combine real ID information with forged document templates and deep fake biometrics to evade customer verification procedures.

Combining Document Verification with Liveliness Checks can detect this kind of fraud as we can spot discrepancies in fake ID documents that natural observers cannot catch.



06. Business Registration Fraud

B2B businesses also deal with their fair share of fraud. A prevalent tactic fraudsters employ involves utilising fake or compromised business registration details to game onboarding systems and create fictitious accounts. This type of fraud can lead to considerable financial losses and undermine user trust if not addressed. Financial services and e-commerce companies are typically the primary targets of such schemes.

Verifying business registration details is a crucial component of our Know Your Business (KYB) solution. This encompasses validating the business name, address, tax information, and identity data of directors, shareholders, and other relevant stakeholders, ensuring a secure and trustworthy environment for all parties involved.



Secure your business: How identity verification helps companies prevent fraud

“ Identity verification is a critical tool in the fight against fraud for any consumer-facing product. Fraudulent users will often try to hide their real identities to get access to systems. Strong identity verification measures discourage a significant percentage of fraudulent users because they have to use their real identities to create accounts. Also, in the event that a user performs fraudulent actions using your product, identity verification measures make it easier to support and comply and law enforcement efforts.”



Elijah Kingson

Chief Product Officer and Co-founder at PayDay

Document Verification: A critical tool for fraud prevention

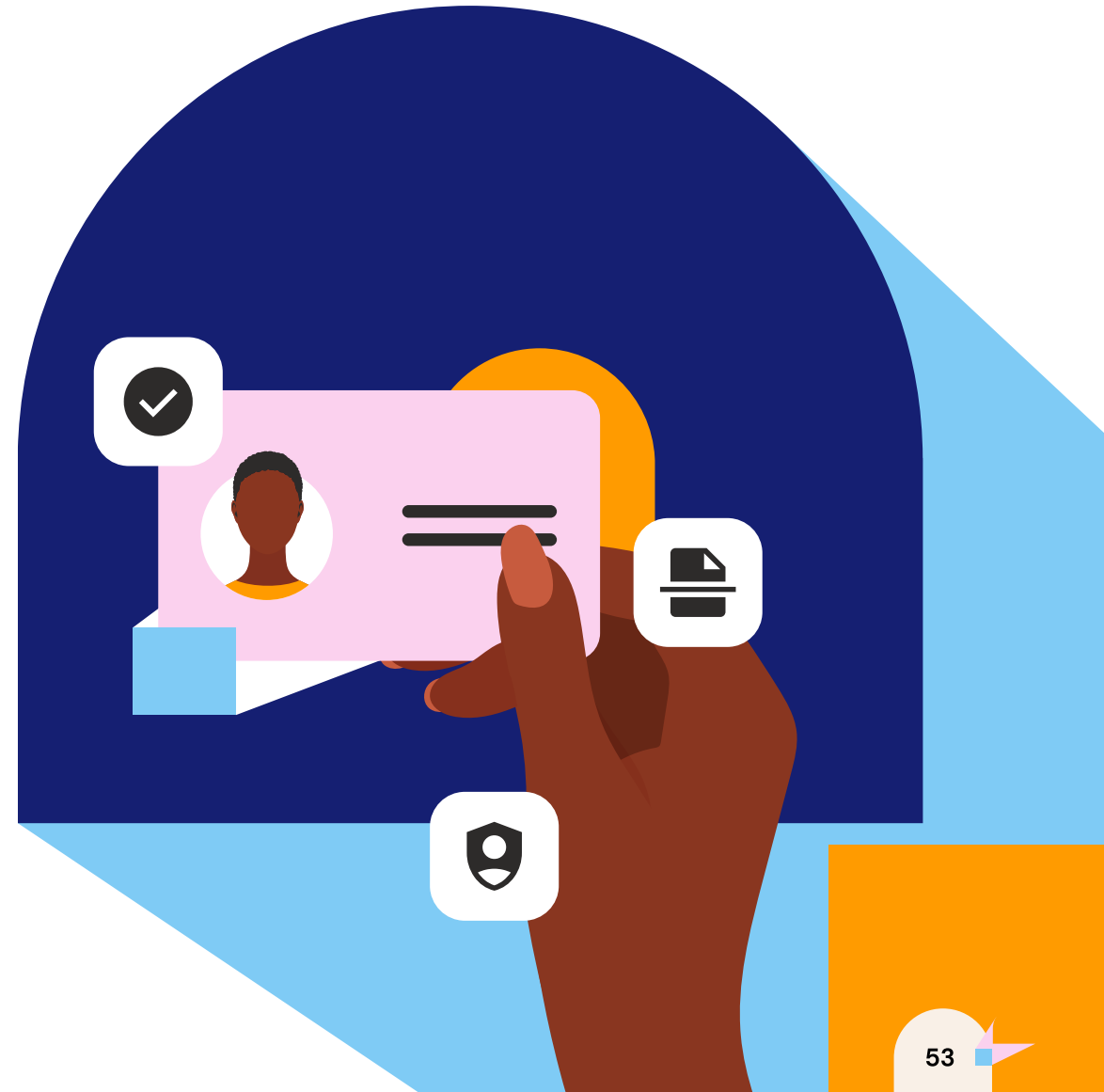
Collecting and verifying user-submitted identity documents, such as driver's licences or passports, is the most common method of KYC globally. Document Verification checks the authenticity of a document and compares the document photo to a selfie.

Smile ID's document verification solution enables you to verify over 8,500 documents across 226 countries globally and the ability to add support for more documents, upon request. We also have true depth of coverage in Africa, with support for at least 3 document types for every African country.

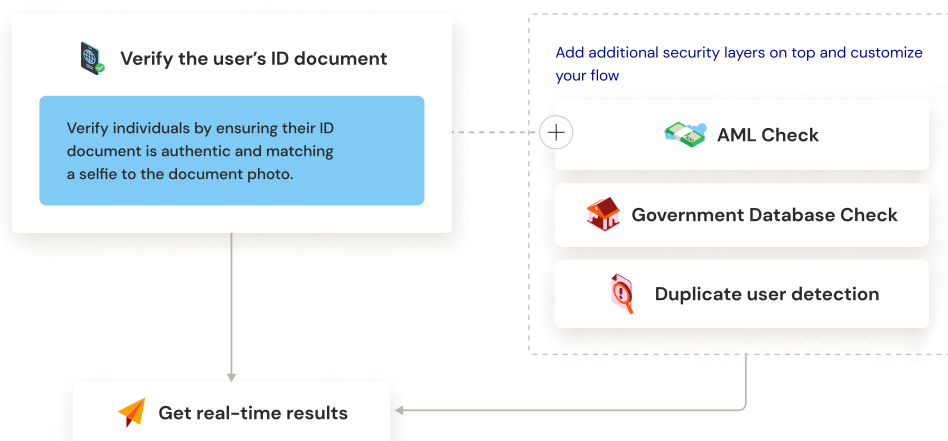
How it Works:

A user submits a photo of an ID document and a selfie, and the following checks are completed:

1. The document will be authenticated to ensure it is a real and valid ID document.
2. Security features on the document, such as barcodes, holographs, and watermarks, will be verified.
3. The photo on the document will be matched to a selfie to verify that the ID belongs to that user.
4. Optical Character Recognition (OCR) reads and returns the textual information on the document.



In addition to helping businesses keep up with KYC requirements and expand into new markets, document verification is critical for keeping out users with forged or stolen IDs. Companies can build a robust anti-fraud solution capable of keeping malicious actors out when combined with other tools like Biometric KYC, Face Deduplication, and AML Checks.



Why Smile ID's Document Verification is the best



Technical integration options for every device and OS combination.



"No Code" solutions for business distribution to users via link, website or email.



3 or more ID types covered in the majority of African markets.

80%

80% user approval rate on key African ID types.



OCR extracted personal information returned with 96% accuracy.



Backed by human review 24/7 at no extra cost improving fraud detection results by 15%.



Switching to Smile ID allowed Bridgecard to achieve a 216% increase in revenue while reducing card issuing downtime by 41%

Overview

- 📊 **Goal:** Pan-African regulatory compliance
- 🏢 **Industry:** Payments
- 📍 **Countries Using Smile:** Angola, Benin, Cote D'Ivoire, Cameroon, Rwanda and more

The Problem

Bridgecard faced multiple challenges in expanding their card issuing services in Africa, including the threat of fraud in the payments industry and difficulties with finding a KYC solution that could perform verifications across multiple African countries

The Solution

Smile ID's document verification solution was invaluable for Bridgecard's expansion, enabling card services in countries with inadequate or non-existent ID databases by verifying users who would have otherwise failed KYC.

Impact

- **41% reduction** in card issuing downtime
- Expansion into **20 markets** across Africa
- **216% increase** in revenue due to expansion & card creation increase
- **57% month-to-month growth** in card creation due to seamless KYC verification process

Testimonial

"We had clients from all over Africa asking if we could provide card infrastructures for customers in their country. With Smile ID coverage across Africa, we were able to scale from 4 to 20 countries in six months."

– Festus Owumi, Chief Technology Officer

Biometric KYC for ID verification

Biometric KYC refers to using biometric characteristics, such as fingerprints, facial recognition, iris scans, and voice recognition, to verify individuals' identity during the KYC process. In recent years, it has emerged as a potent tool for combating fraud, particularly as criminals increasingly find ways to obtain or fabricate valid ID numbers that can pass conventional text-based ID verification.

Biometric traits are unique to individuals, making them difficult to replicate or forge. Unlike passwords which can be forgotten, stolen, or shared, biometric data is inherent to each person and remains constant.

Biometric KYC systems have advanced algorithms that analyse and compare biometric data to identify anomalies and inconsistencies. By cross-referencing biometric information with existing databases, these systems can detect patterns associated with fraudulent activities, such as multiple registrations under different names or attempts to manipulate biometric features. Suspicious activities can be flagged and investigated, preventing fraud before it occurs.



Why selfies are the go-to choice for biometric authentication

Even though other options have merits, facial recognition has become the preferred biometric KYC method worldwide in recent years.

The accessibility of facial recognition technology serves as a key factor in its widespread adoption. Specialised equipment is often required for fingerprint, iris, and voice recognition, making them less accessible. In contrast, facial recognition is easily performed using the front and back-facing cameras found on most smartphones, allowing users to access the technology anytime, anywhere. Additionally, the popularity of the "selfie-style" picture format among smartphone users presents a non-intrusive, user-friendly way to capture facial biometric data.

Increased security also contributes to facial recognition technology's popularity. Although all biometric data is unique to each individual, some forms are easier to fabricate than others. AI-generated voices can deceive voice recognition software by closely mimicking an individual's voice. Fingerprint recognition software has proven to be easily bypassed as well. In contrast, facial recognition programs are the most difficult to circumvent, as they can incorporate liveness checks and anti-spoofing technology to ensure the user's authenticity.

Smile ID's Biometric KYC

Smile ID has been at the forefront of leveraging Biometric KYC for remote onboarding across Africa, enabling our clients to rapidly and securely scale their user base to millions. Our Biometric KYC solution at Smile ID involves matching a user's submitted selfie with the photo on their Government-issued ID documents.



This approach combines the reliability of document verification with the added assurance of biometric comparison, ensuring that your users are indeed who they claim to be.

To achieve this, we utilise our proprietary facial verification technology called SmartSelfie™, which is coupled with document verification. This combination allows for a de-biased and highly accurate comparison between a user's selfie and the image on their identification document.

Liveness checks using SmartSelfie™

A strong anti-spoof system should back up biometric checks to ensure customer safety. While sophisticated attacks like “deep fakes” are still relatively uncommon in Africa, so-called “cheap fakes” are prevalent. These include photos of screens, uploading static photos, or wearing masks. These types of fakes can easily be prevented with a liveness check. Liveness algorithms complement and augment face recognition, resulting in robust onboarding that users understand and app developers can trust.

Many apps that leverage liveness detection capture a short video of the user during registration. Alternatively, some apps grab a quick succession of frames and/or audio while the user performs a specific motion or gesture. The liveness solution processes the visual/audio data with specialised algorithms, generating a mathematical confidence score on whether a real human was present during image capture. Humans can review and label results for further algorithm training and refinement.

At Smile ID, we have been working on face recognition and liveness solutions since 2016. Our trademarked technology – SmartSelfie™ – uses 6 AI-based models and is backed by real-time reviewers that label thousands of images daily for machine learning purposes. SmartSelfie™ technology powers our mobile and web solutions.





Yellow Card automates KYC in 16 countries while complying with KYC/AML requirements

Overview

- 📊 **Goal:** Pan-African regulatory compliance
- 🏢 **Industry:** Crypto
- 📍 **Countries of Operation:** Botswana, Cameroon, Malawi, Côte d'Ivoire, and 12 more

The Problem

Crypto companies face a high degree of regulatory scrutiny but conforming to varying regulations while operating in many markets can be complicated.

The Solution

Using a mix of KYC solutions including **document verification, government database checks and biometrics face matching** has allowed Yellow Card to stay compliant while scaling into 16 countries and counting.

Impact

- Became **first licensed** crypto provider in Botswana
- Digitally verified **300M+ users**
- Scaled to **16 countries** across Africa

Testimonial

"Working with Smile has improved our KYC in key markets but also as we expand across Africa. Together, we have solved problems customers are dealing with from a mobile device that can't take a picture clearly to how quick we can get information stored and vetted. It's been quite amazing to work with the Smile ID team."

– Mandy Naidoo, Chief Compliance Officer

Face Deduplication

Fraudsters that create multiple accounts to collect promotional rewards or loans are committing a duplication attack. These efforts are usually only worth it for the attacker if they can successfully sign up for many accounts. While fraudsters have found ways to infiltrate ID systems and generate multiple ID numbers, it is much more difficult for them to alter their face. Biometric de-duplication performs a one-to-many search (1:N), looking for a single face among thousands or millions of other faces.

Deduplication is a potent tool to prevent duplicate account fraud. In practice, deduplication searches a history of faces that have been previously onboarded and alerts you if the same face is attempting to sign up again. This will flag a duplicate sign-up regardless of country, ID type, ID number, name, or date of birth. Deduplication is the most effective deterrent for organised attacks on promotional sign-up codes.

Smile Secure from Smile ID is our proprietary tool that stops duplication fraud. It scans new incoming selfies in real-time during onboarding and notifies you in seconds if an incoming face has been onboarded to your service in the past, regardless of ID type. To date, Smile ID has detected over 1.7 million duplicate faces for our customers & Smile Secure was able to identify and surface these repeat attempts.

Contact us to learn more.

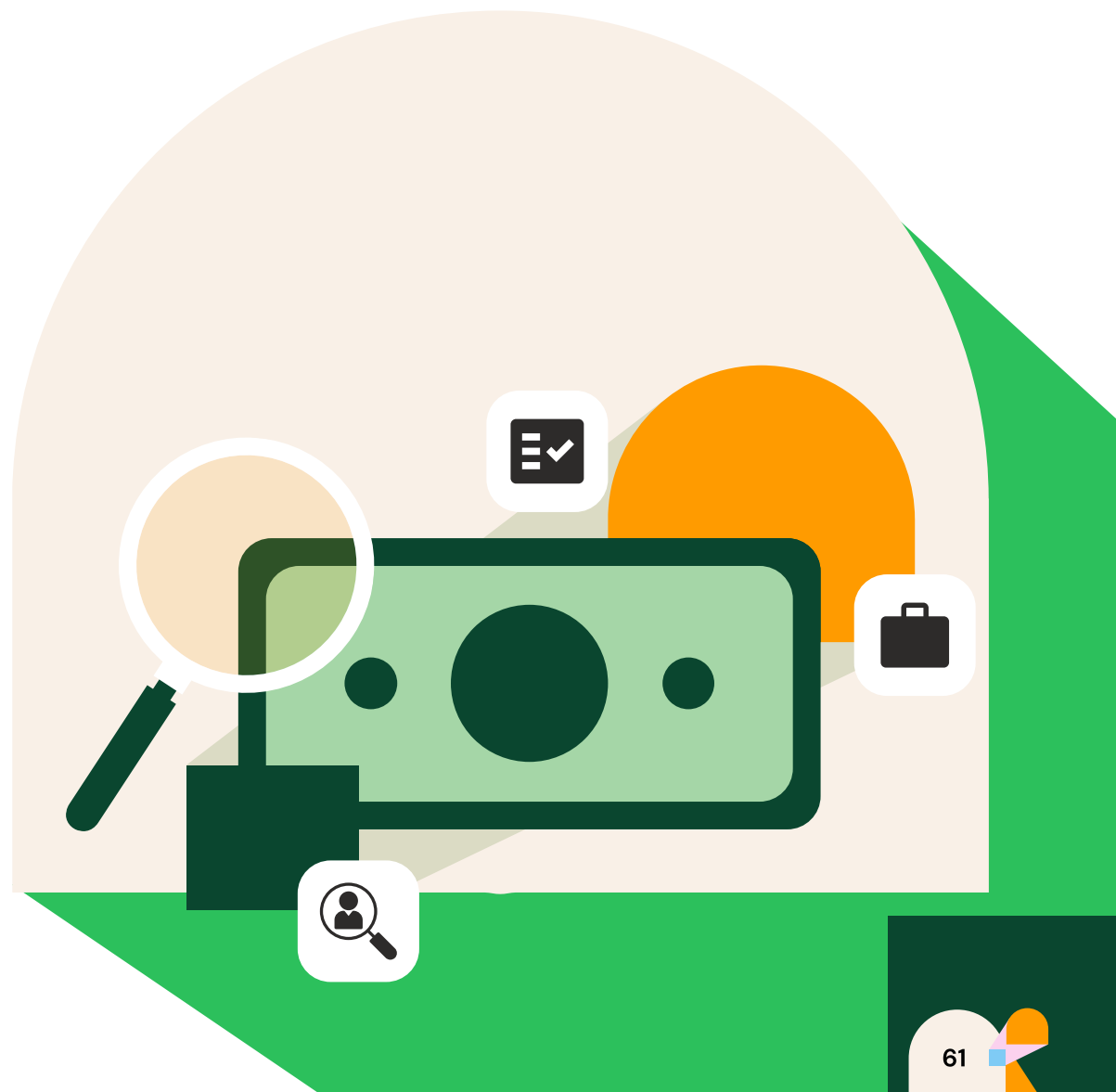


AML Check

AML due diligence is a crucial business compliance requirement, particularly when dealing with politically exposed persons (PEPs). It identifies and filters high-risk customers who may be listed on sanction lists, political watchlists or even mentioned in adverse media. These higher-risk customers, especially those on sanction lists, are more likely to require close monitoring through Enhanced Due Diligence (EDD) measures. By identifying these potential threats, businesses can take appropriate actions, such as blocking them or implementing enhanced KYC checks.

AML Checks are an effective tool in preventing fraud or misuse of your products by identifying users who with higher risk profiles, as they allow businesses to compare customer details against sanction lists to assess their level of risk.

Smile ID's AML Check enables businesses to conduct due diligence on customers by swiftly screening them against over 1,100 global watchlists, lists of politically exposed persons, and adverse media publications. Within seconds, the product provides information on whether the screened customers are found on any of these lists, along with corresponding details. This information can then be utilised to evaluate the associated risks the customers pose.



Know Your Business

Know Your Business (KYB) procedures are imperative for B2B service providers who face a wide range of fraud-related threats, including business identity fraud, money laundering, and sanction violations. B2B service providers must verify that the businesses they serve are who they say they are, do what they say they do, and are owned by the people they claim to be owned by.

Smile ID's KYB solution helps B2B businesses conduct due diligence on corporate clients. More than just verifying the business registration names and numbers, we help companies verify the identities of beneficiaries from the business. Our KYB solution takes the customers' business registration number and returns due diligence information, including business registration name, tax number, shareholder, director, and beneficial owner information.



How to protect yourself from ID-related fraud

Identity verification on peer-to-peer platforms is both a security feature and a compliance requirement. Verified users are less likely to be fraudulent, so a user's verification status signals trust. It's best to avoid transacting with unverified accounts as they carry a higher risk for fraud.



01

Share information with caution

Scammers use tactics like phishing and impersonation to trick individuals into revealing personal identification details. This stolen information can be used to access victims' accounts. Therefore, it's vital to share identity-related information only with reputable organisations. Legitimate entities won't request sensitive details via unsolicited calls or emails. If a request seems suspicious, it's best to decline and contact the organisation through official channels to confirm its authenticity.

03

Obtain and review your credit report regularly

Identity theft can result in fraudulent accounts and unauthorised loans that damage your credit rating. To prevent this, review your credit report annually for any inaccuracies or suspicious activities. Early detection allows for immediate action, helping to protect your credit score from potential harm.

02

Monitor accounts for suspicious activities

If you notice suspicious activities like unfamiliar logins or unauthorised transactions on your accounts, it might indicate a compromise. Regularly reviewing your financial statements can help detect such activities. If you spot anything unusual, report it to your financial institution immediately. Stay vigilant, frequently change passwords, and use unique, strong passwords for each account to minimise the risk of identity theft and financial loss.

04

Avoid transacting with unverified accounts where possible

Identity verification on peer-to-peer platforms is both a security feature and a compliance requirement. Verified users are less likely to be fraudulent, so a user's verification status signals trust. It's best to avoid transacting with unverified accounts as they carry a higher risk for fraud.

05

Report stolen/missing ID documents as soon as noticed

Report stolen or missing identity documents to authorities and financial institutions immediately to prevent fraudulent use. Reporting can aid in recovering or replacing the document and protect against nefarious activities, as a significant percentage of fraud is facilitated by stolen IDs.





Contributors

**Megan
Keirstead**

Product Marketing Manager

**Lameck
Orina**

Graphic Designer and Illustrator

**Navid
Scheybani**

Chief Growth Officer

**Kai
Tyng Loh**

Head of Analytics

**Mark
Straub**

Chief Executive Officer

**Peace
Itimi**

Director of Marketing

**Orahachi
Onubedo**

Content Writer



Remotely verify individuals & businesses in seconds

Stay KYC/AML compliant & prevent
fraud at scale.

CONTACT US

usesmileid.com/talk-to-an-expert

 **Smile ID**