H1 2022 REPORT

State of KYC in Africa

SMILE IDENTITY

Contents

Foreword:

Our Shared Vision of the Future

The growth of our business has coincided with a movement across Africa to reimagine digital identity as an ecosystem of APIs and consent-driven software, rather than physical IDs and expensive hardware. This trend, pioneered by governments in emerging economies and backed by international development institutions, has resulted in new digital infrastructure and data protection policies that unlock inclusive growth.

These building blocks have enabled us to innovate and build rapid onboarding and verification solutions for critical services like agriculture, banking, payments, savings and investment. We are grateful to our partners in the public sector. Together a community of stakeholders across technology, business and government are building trust in Africa, and for Africa, throughout the world.

At Smile Identity we believe anyone should be able to prove their identity online, regardless of the origin of their ID card or IP address.

Over the past 5 years, our Pan-African experience has given us a unique vantage point from which to compare the performance of existing digital ID infrastructure. In publishing this, our inaugural report, we seek to share learnings and showcase how success in one market can translate to the next. We take into account the unique demographics, ID types, infrastructure and compliance rules of each country.

We aim to accelerate the adoption of ethical digital identity systems connecting Africa to the world.

Smile Identity's growth, as shown in this metrics report, is a function of our expertise in the African market and technology optimized for the continent. In this, our inaugural report, we provide an in-depth look at our focus markets in order to approximate the growth and development of digital KYC across Africa.

This report uses anonymized data collected from transactions on Smile Identity's production environment. It is our best effort to reflect trends on the African continent but may not reflect every market.

Africa’s digital transformation is happening fast.

As the continent continues to develop, it is becoming increasingly digital. Key drivers of this advancement are increased Internet and mobile phone penetration, and a young population. With a median age of 19.7 years, many Africans are digital natives, just now entering the workforce.

The continent has 690 million mobile subscribers, a penetration rate of over 60% and growing.

Similarly, the number of Internet users has increased to 523 million. And in 2022, for the first time Internet penetration crossed 51% in two of our focus markets (Nigeria and Ghana). This has enabled businesses to reach a wider audience and tap into new markets. A lot of technology startups have cropped up to solve some of Africa's key problems and are rapidly preparing for pan-African expansion.

Source: Google/IFC e-Conomy Africa report

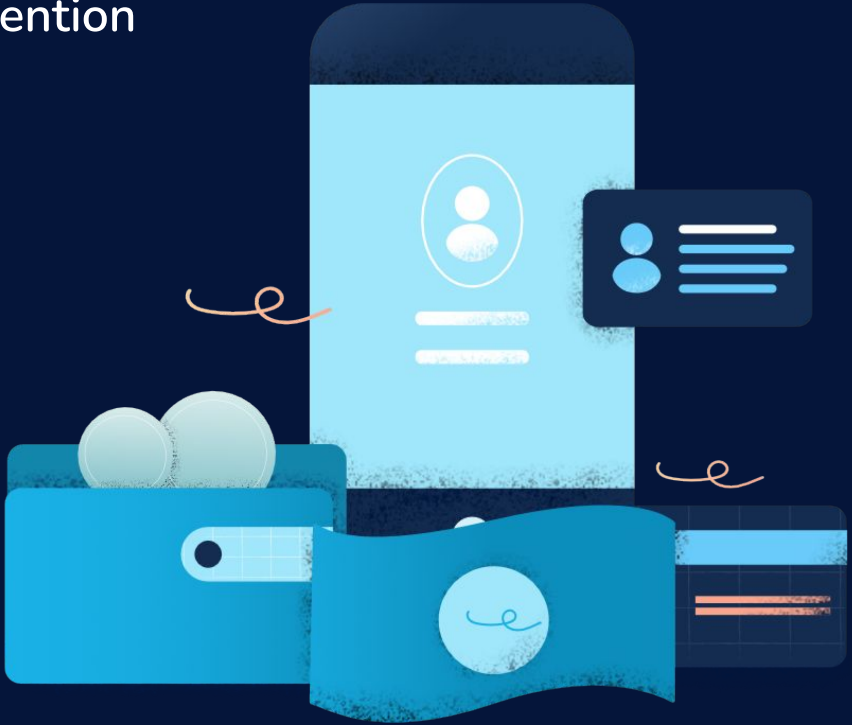
Fintech services are attracting a lot of attention

Fintechs and mobile money have become powerful growth drivers in Africa, responsible for 2/3rds of all financial accounts, outpacing banks, and attracting billions of dollars of investment. Fintech alone was responsible for 75% of all venture capital investment into Africa in 2021.

Consumers and businesses are adopting mobile money, digital wallets and cryptocurrency to make it easier to send, receive, and use money. But these services are also attracting the attention of bad actors.

Fraudsters are mounting more frequent attacks and undermining basic KYC checks with social engineering, stolen IDs and duplicate accounts.

This is resulting in higher reported fraud and losses, bringing scrutiny from regulators.



Source: Google/IFC e-Conomy Africa report. Partech Africa Investment Report. Central Bank of Nigeria

Key Takeaways

Fraud attempts increased by more than 50%

In the last two years, fraud attempts increased by 50%. The first half of 2022 alone saw a 30% increase over 2021. There has been a noted increase in countries like Kenya and a reduction in observed fraud attempts in Ghana and South Africa.

Most fraud is unsophisticated, for now...

The majority of the fraud attempts we've seen have been of low sophistication - i.e. attempting to open an account with a stolen or invalid ID. But as the value at risk increases, fraudsters are attempting complicated hacks like poisoning of identity databases with fake names and faces.

Digital identity infrastructure in Africa is improving

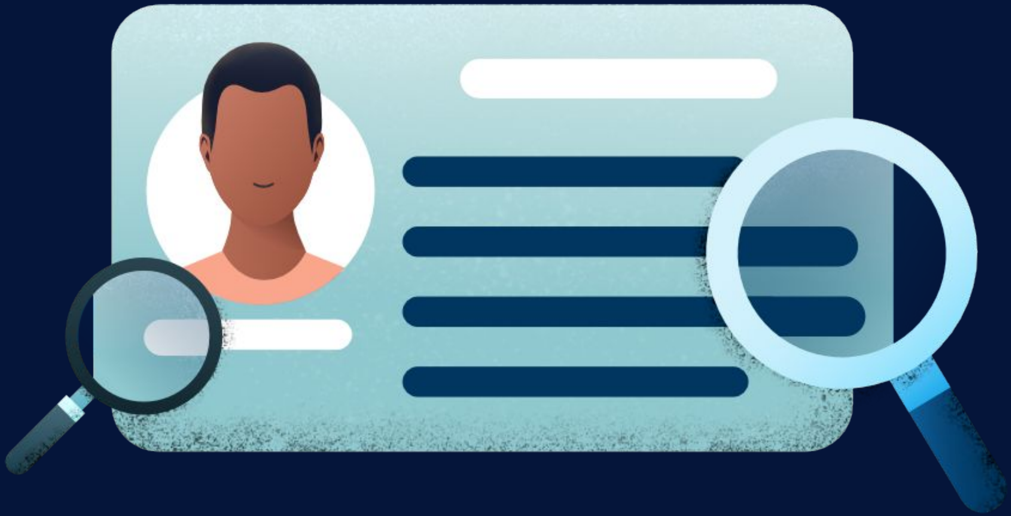
Several African countries are updating their digital identity infrastructure. Nigeria and South Africa are encouraging their citizens to enroll in more secure IDs that centralize and standardize information. Kenya, on the other hand, is still seeking judicial approval for the use of its new Huduma Namba ID.

Not all industries affected equally by fraud

Buy Now Pay Later (BNPL) companies are seeing high rates of fraudulent attempts as fraudsters try to get away with more opportunistic crimes. On the other hand, crypto companies in Africa are noting lower fraudulent attacks than expected.

The Importance of KYC

The "Know Your Customer" (KYC) process is a requirement that helps businesses identify their users and verify their credentials.



There are two reasons for conducting KYC checks:

1. Regulatory compliance
2. Fraud prevention

KYC allows companies to identify risks associated with individual customers before they happen. Central banks often require KYC checks to prevent financial crimes like money laundering. For fintechs, online payments companies and ecommerce, KYC can prevent fraud.

In order to comply with KYC regulations, businesses collect information from their customers, including name, date of birth, and ID number. They may also require additional information such as address, proof of income or employment. Companies then verify this information using reliable sources.

This process can be time-consuming and expensive but the Internet and mobile phones have allowed businesses to reimagine their customer onboarding journeys. Many are turning to technology to streamline these processes, making compliance easier and improving customer experience.

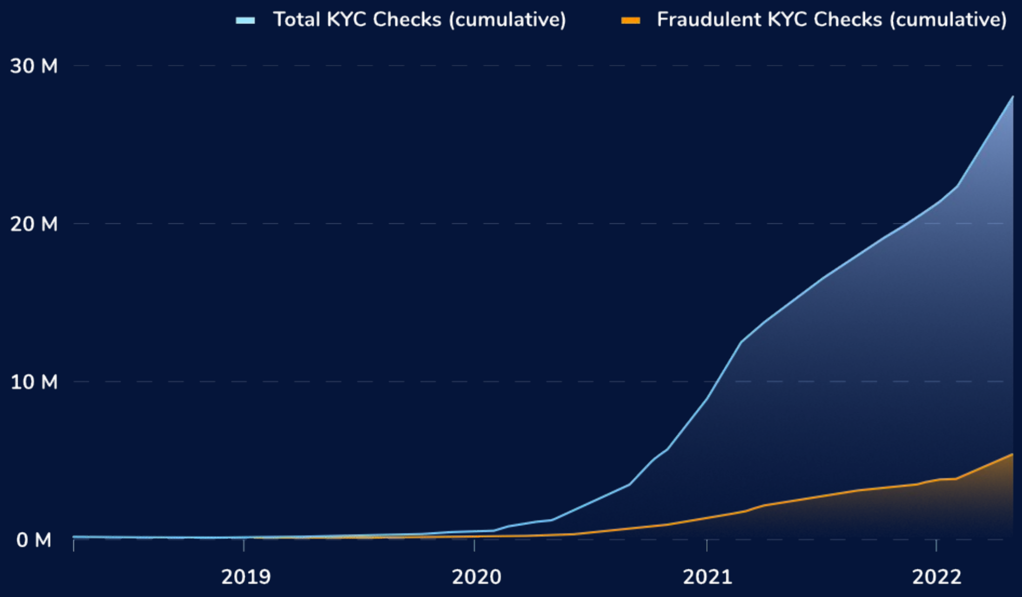
“Biometric KYC” can assist by confirming that the person providing a credential (an ID number), is in fact, who they say they are. Biometric systems that use deduplication can also be used to to ensure a person is in fact, ***only who they say they are.***

Recent Trends & Insights in Africa

H1 2022

KYC Checks by Smile Identity

Cumulative checks over time



Note on chart and data set: This report uses anonymized data collected from transactions on Smile Identity. Fraudulent KYC checks include biometric Fraud and data validation errors when checking against the government ID database

Remote onboarding is taking off in Africa

As more services move online, KYC and onboarding is becoming mostly remote. Instead of having users show up physically to provide credentials, many African businesses are conducting the entire process through a web or mobile interface. In some cases, agents are extending the reach of online services by visiting users who do not have smartphones.

Since 2019, we have run 30 million KYC checks, with exponential growth noted during the pandemic period. As such, we have developed a insights and pattern recognition about fraudulent activity happening in the digital space.

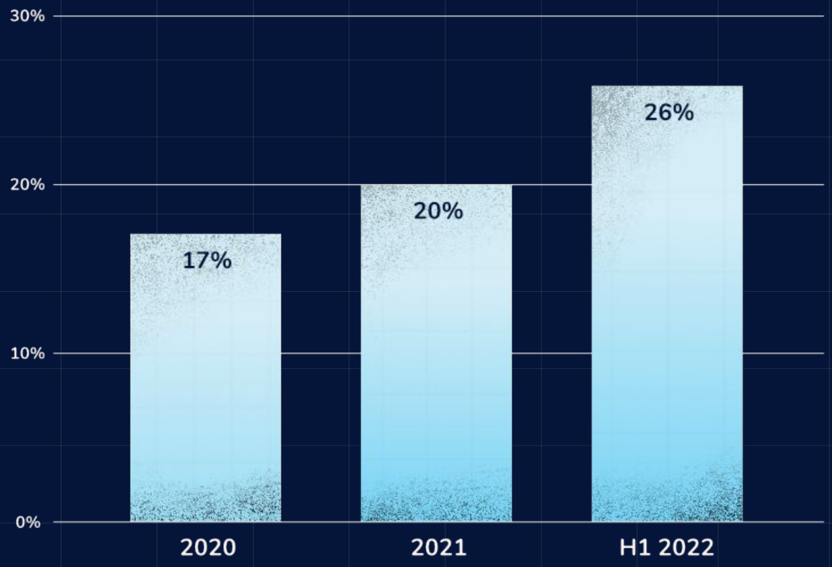
Fraud attempts have increased by more than 50% in the last two years

In early 2020 during the pandemic, we saw a shift towards remote onboarding, which, while faster, initially lacked the same checks present during physical onboarding. Cybercriminals and fraudsters capitalized on this shift, emboldened by the perceived 'anonymity.'

In 2020, 17% of all Smile Identity KYC checks were flagged as attempted fraud. In the first half of 2022, we saw this number increase to 26%. For the foreseeable future as businesses adapt to the new virtual reality, we expect to see more and new types of fraud emerge on an increasing basis.

Fraudulent attempts caught by Smile Identity

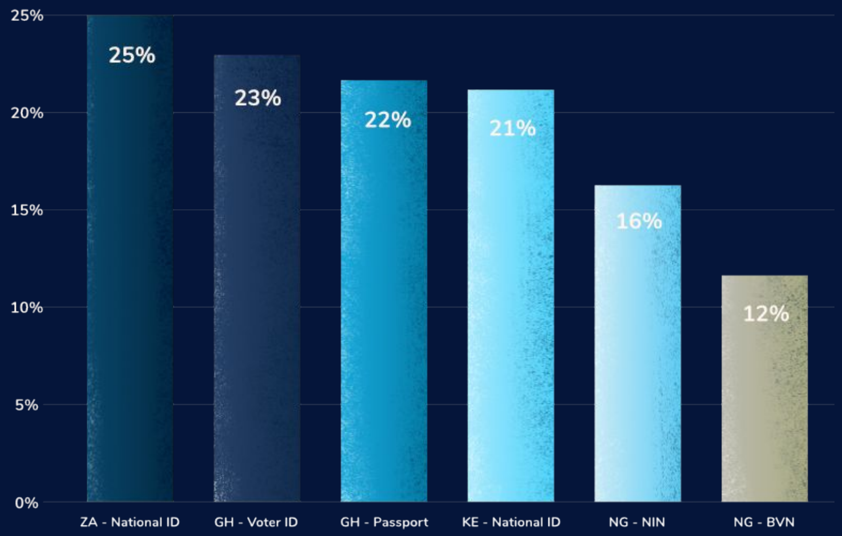
% of Total KYC Checks



Note on chart and data set: This report uses anonymized data collected from transactions on Smile Identity. Fraudulent KYC checks include biometric Fraud and data validation errors when checking against the government ID database

Biometric Fraud attempts caught by Smile Identity

% of Total KYC Checks, by ID Type



Note on chart and data set: This report uses anonymized data collected from transactions on Smile Identity. Biometric fraud rates are measured by Smile Identity between January and June 2022; includes approximately 12 million KYC checks across Africa; selected countries and ID types with significant volumes

Fraudulent attacks using government-issued documents

Across Africa, there are various identity documents used for identity verification. The national ID is the most common in many markets. These IDs are used to gain access to products and services across government and the private sector alike.

We see varying degrees of fraud attempts depending on our clients' activity, size, location, and industry. Promotional offers tend to attract more fraud attempts as bad actors try to game the system in order to reap promotional rewards. We saw a lot of promotional campaigns coming from South Africa in the first half of the year, with some of our clients entering the country and attempting to attract customers to their service.

Fraud trends by country

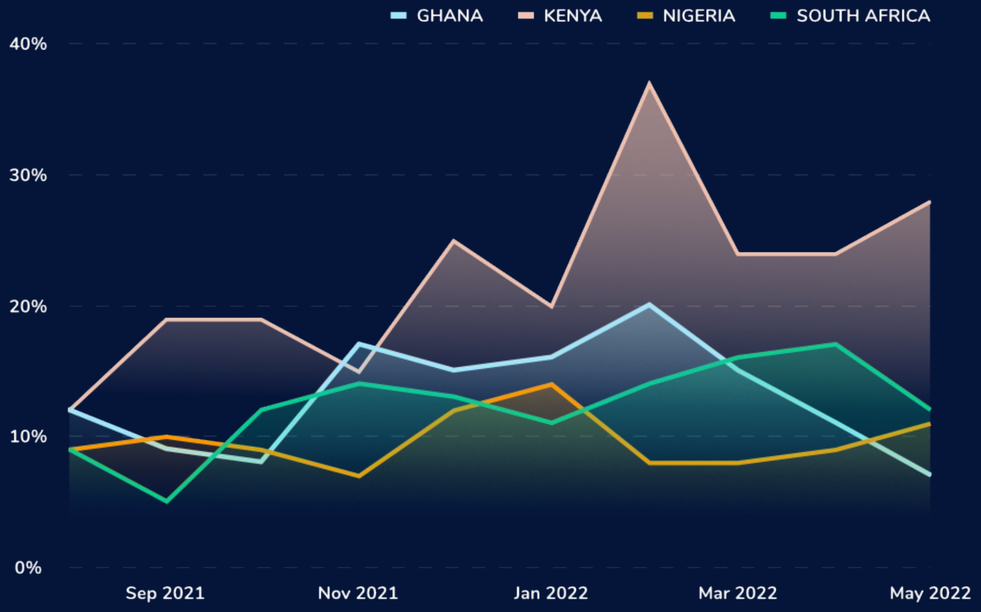
The use of biometrics has become part of everyday life, be it unlocking your phone with your face, accessing office buildings with a fingerprint or clearing customs at the airport. Its pervasive use has made it attractive to adopt due to the shallow learning curve required.

As such, governments across Africa have been adopting biometrics for their new and improved national ID systems. For example, Ghana has released their new Ghana card, which consolidates information from tax identification numbers and ID numbers into a single card with a chip.

As countries see a wider adoption of their improved digital ID systems we see a stabilization in the number of biometric fraud attempts. Countries with lower adoption of biometric IDs may notice fluctuations in fraud as less modern systems provide more avenues for attack.

Biometric Fraud attempts caught by Smile Identity

% of Total KYC Checks, by country



Note on chart and data set: This report uses anonymized data collected from transactions on Smile Identity. Biometric fraud rates are measured by Smile Identity between January and June 2022; includes approximately 12 million KYC checks across Africa; selected countries and ID types with significant volumes

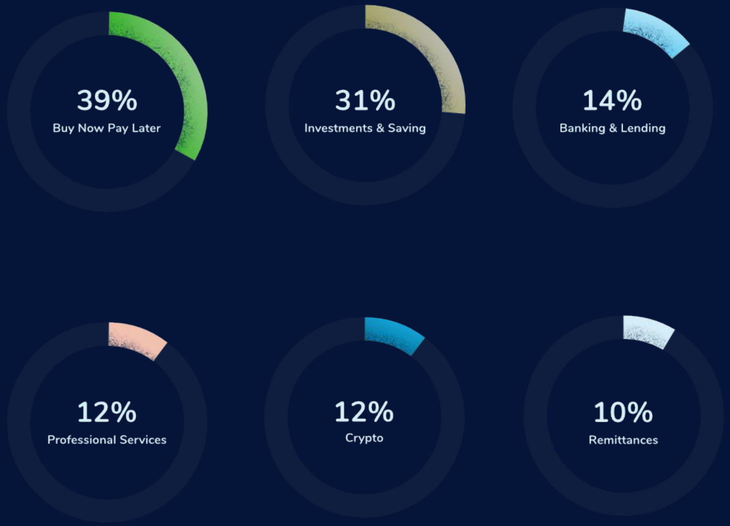
Fraudsters are more frequently targeting buy now pay later platforms

While we see bad actors attempt to infiltrate platforms in every industry, some are worse than others. Generally, fraudsters put in effort where the rewards are the highest.

At Smile Identity the highest rates of attempted fraud we see are in the buy now pay later (BNPL) sector. The value at risk if a bad actor successfully impersonates another person is relatively high. A fraudster who beats the system just 1 time can make off with high value goods. In comparison in other industries, the value at risk may be a small referral fee that only becomes attractive to a fraudster if they can collect it over and over.

Biometric Fraud Rate by Industry

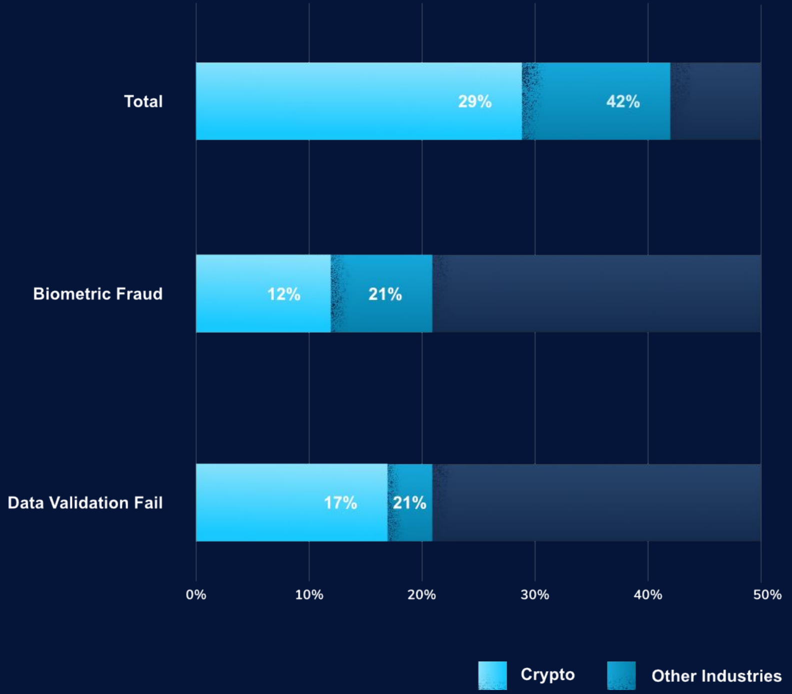
% of total within industry; Africa average



Note on chart and data set:
This report uses anonymized data collected from transactions on Smile Identity between January and June 2022; includes approximately 12 million KYC checks across Africa; selected countries and ID types with significant volumes

Fraud Rate of Crypto vs Other Industries

% of total within industry; Africa average



Despite an increase in usage, crypto platforms are seeing lower than average fraud at sign-up

In 2021, Smile Identity processed over 1.3M KYC checks for our partners in the crypto industry. This was a 55% increase over the previous year. As crypto exchanges continue to grow, so do concerns around safety.

Large, difficult to trace, high-profile scams have plagued the crypto market often giving them a notoriously bad reputation and intense scrutiny from regulators. Yet, Smile Identity's data shows that the crypto platforms conducting KYC on with our system are actually reporting a lower rate of attempted fraud than other industries.

Based on our data, crypto platforms have also seen less sophisticated attacks. Data validation failures, like providing fake or stolen ID numbers, are more common than biometric spoofs.

When a fraudster successfully attacks a crypto platform and compromises existing wallets, the impact can be devastating, but our data suggests high-impact attacks on existing wallets are not indicative of a higher frequency of fraud during account opening.

Note on chart and data set:
This report uses anonymized data collected from transactions on Smile Identity between January and June 2022; includes approximately 12 million KYC checks across Africa; selected countries and ID types with significant volumes

ID database downtime affects real-time KYC services

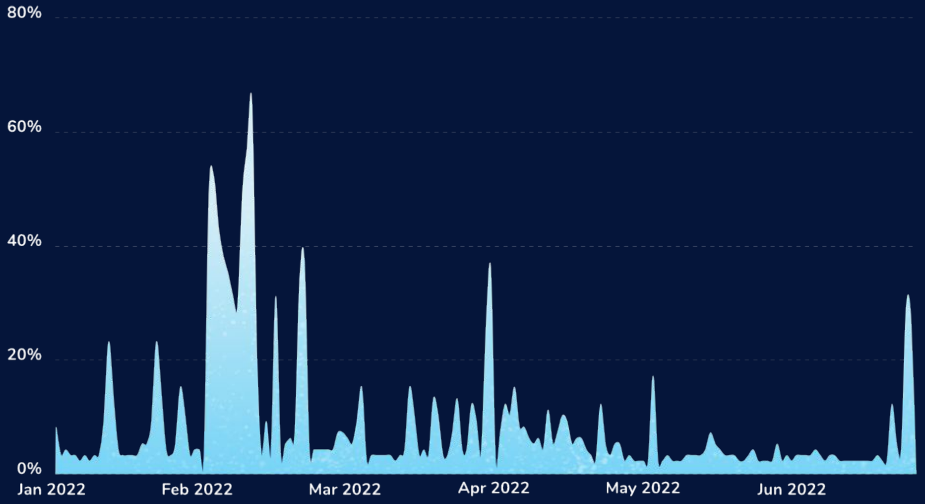
Identity verification services rely on connections to ID authorities as their source of truth. However, the volatility in ID database uptime is a significant obstacle for real-time verification. Depending on how long an ID database outage lasts, it may have a substantial effect on KYC services.

In early 2022, we observed frequent unscheduled ID database outages, which disrupted the ability to verify IDs. **Overall, ID databases were offline 9% of the time**, leading to thousands of checks waiting in queues or needing to be re-run.

With significant investments being made to Africa's digital identity infrastructure, we expect to see this problem decline. Partnerships between government, development institutions and the private sector are driving change and reducing downtime. The second quarter of 2022 witnessed a noticeable improvement in the reliability of major ID types.

Daily ID Database downtime

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



	Q1	Q2
Average Downtime	9%	3%
Max Downtime	63%	34%
Days w/ 10%+ Downtime	23	6

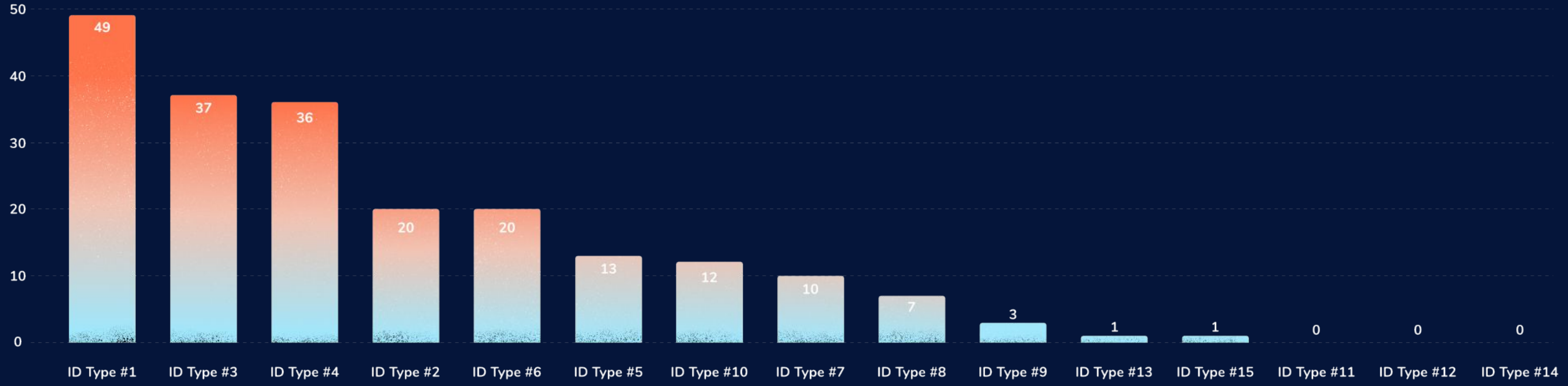
Note on chart and data set:
This report uses anonymized data collected from transactions on Smile Identity between January and June 2022; includes approximately 12 million KYC checks across Africa; selected countries and ID types with significant volumes

Some ID types experience more frequent downtimes

When we drill down into the specific ID types, we see that some have more downtime than others. This means that end users attempting to sign up for or gain access to a platform using these ID types are unable to progress until the database is back up and running. In the last six months, the ID type with the most downtime had 49 days with more than 10% downtime between January and June (H1 2022; 180 days). Smile Identity clients are able to rotate between popular ID types to minimize interruptions to their end users.

Days with more than 10% Downtime

During 180 day period from Jan to Jun 2022; measured by the % of KYC checks that could not be completed;



Get in touch with us to find out more about ID database downtimes and how to improve the consistency of your service.

Note on chart and data set: This report uses anonymized data collected from transactions on Smile Identity between January and June 2022; includes approximately 12 million KYC checks across Africa; selected countries and ID types with significant volumes

Country Deep Dives

Nigeria, South Africa and Kenya

Spotlight: Nigeria

Nigeria has a more robust ID system than many other countries. The IDs issued in Nigeria are generally well adopted with accurate data and good images that can easily be used for automated identity verification.

POPULATION
212 Million

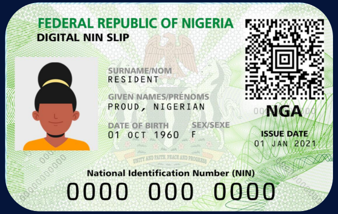
% OF POP WITH ID
50%

MEDIAN AGE
18

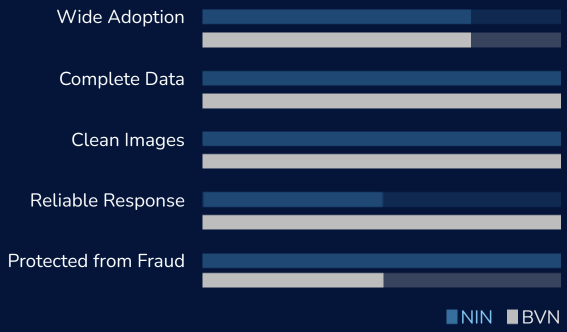
PRIMARY ID ISSUER
National Identity Management Commission

Sources: *CIA World Factbook Nigeria, World Bank ID4D Global Findex Survey*

Nigeria ID Authority



FEDERAL REPUBLIC OF NIGERIA
DIGITAL NIN SLIP
SURNAME/NOM
RESIDENT
GIVEN NAMES/PRENOMS
PROUD, NIGERIAN
DATE OF BIRTH 01 OCT 1960
SEX/SEXE F
NGA
ISSUE DATE
01 JAN 2021
National Identification Number (NIN)
0000 000 0000



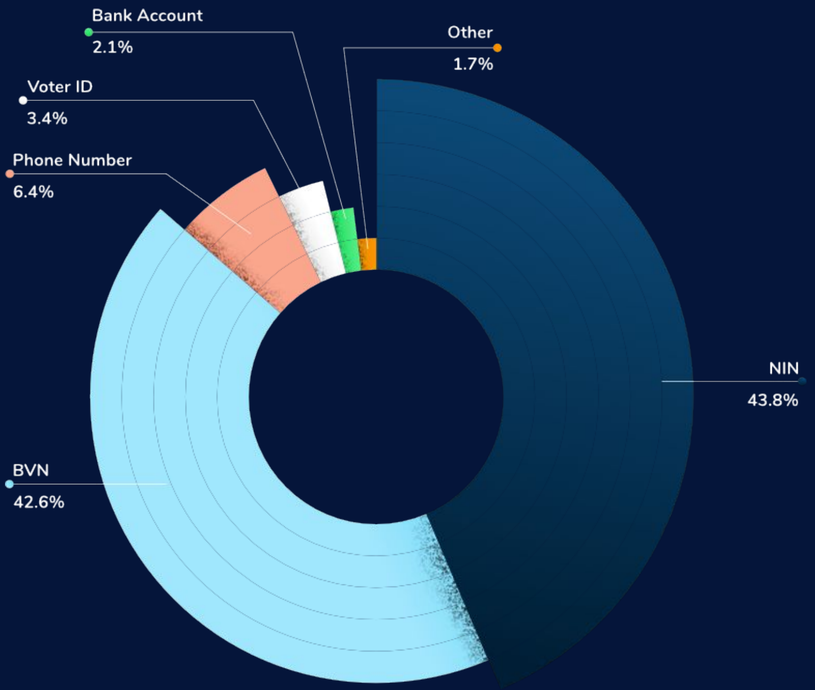
Compliance Rules for Data Access

The Nigerian Data Protection Regulation (NDPR) is the primary data protection framework in Nigeria. To query identity information under NDPR it necessary to comply with policies including; soliciting explicit consent for the processing and cross-border transfer of personal data and ensuring the right of erasure.

To process BVN information the Central Bank of Nigeria(CBN) also requires your business to be a licensed entity in the country.

Smile Identity complies with the NDPR as a data processor in Nigeria and acts as a Payment Solution Service Provider in accordance with the CBN.

Share of ID Types Used



KYC checks reflect a greater adoption of NINs

When Nigeria lacked a robust National ID system, the Bank Verification Number (BVN) which was introduced by the Central Bank of Nigeria, became the most commonly used ID online. However, in recent years things have started to change.

The National Identification Number (NIN) has now registered 85 million Nigerians. Just in the last year, 31 million new registrants were enrolled into the system.

This large adoption is partly due to a policy implemented by the Nigerian government which mandated that SIM cards be linked to an NIN. This has pushed many Nigerians to register for an NIN in order to access mobile services.

We have seen this effect in KYC checks as well. In 2021, more users submitted an NIN for their Smile Identity KYC check than any other credential.

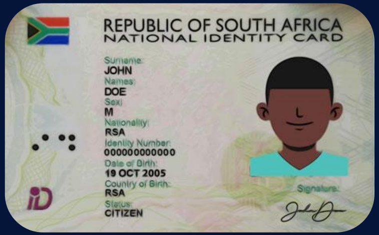
Note on chart and data set:
This report uses anonymized data collected from transactions on Smile Identity between January and June 2022; includes approximately 12 million KYC checks across Africa; selected countries and ID types with significant volumes

Spotlight: South Africa

The National ID is the dominant ID type in South Africa, covering about 40 million individuals. The Department of Home Affairs has implemented a robust database around the National ID. It has nearly universal adoption with 92% of the population above 15 obtaining a National ID and has high quality photos registered.

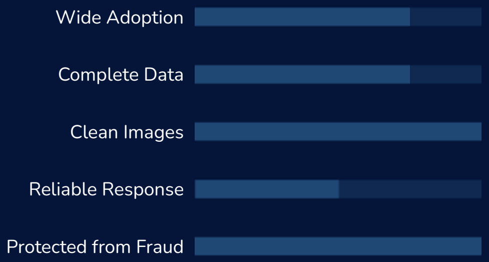
POPULATION	POP 15+ WITH ID
57.5 Million	**92%**
MEDIAN AGE	PRIMARY ID ISSUER
28	**Department of Home Affairs**

National ID ZA



REPUBLIC OF SOUTH AFRICA
NATIONAL IDENTITY CARD

Surname:
JOHN
Names:
DOE
Sex:
M
Nationality:
RSA
Identity Number:
0000000000000
Date of Birth:
19 OCT 2005
Country of Birth:
RSA
Status:
CITIZEN
Signature:

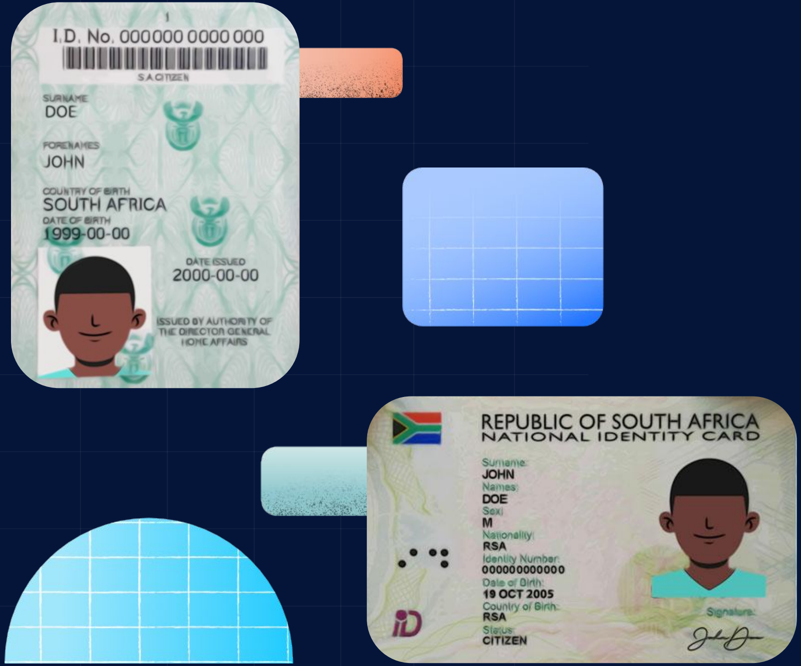


Compliance Rules for Data Access

The Protection of Personal Information Act (POPIA) provides the overarching framework for processing the personal data of residents of South Africa. POPIA requires Responsible Parties (data controllers) to be registered with the Information Commissioner in South Africa and to collect explicit consent before personal data is processed or transferred out of South Africa.

Smile Identity is registered as a Responsible Party in South Africa and processes identity information in compliance with POPIA.

Sources: CIA World Factbook South Africa, World Bank ID4D Global Findex Survey



A Tale of 2 ID Documents

The National ID is the dominant ID type in South Africa, however, this document comes in 2 formats. The older version is known as the "green book" and the newer document is a "smart ID card."

The new smart ID card has several security features and is difficult to forge, unlike the green book. It has two means of authentication, a fingerprint and password known only to the user, and a variety of other safety mechanisms including a microchip.

Today, the South African green book remains in circulation but is being phased out as the Department of Home Affairs undertakes a major drive to instate the new smart ID card. While the replacement drive started in 2013, the smart ID is not yet widely distributed.

New IDs are issued as smart ID cards. South Africans will also get the new smart ID cards as a replacement for the green book. However, neither the green book nor the smart ID card have an expiration date so they will only be replaced if lost or damaged.

Spotlight: Kenya

The National ID is the primary ID type in Kenya, covering 29 million individuals. While it is widely adopted, the database is missing photos for roughly 40% of individuals registered.

Missing photos and challenges with intermittent downtime make this API unreliable when used alone. Smile Identity's Biometric API uses the system in conjunction with document verification checks to enable better onboarding outcomes.

POPUPLATION

55.8 Million

POP 18+ WITH ID

91%

MEDIAN AGE

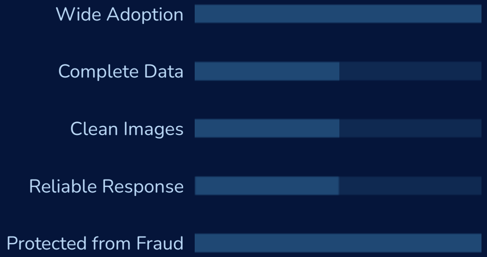
20

PRIMARY ID ISSUER

Integrated Population Registration System

National ID KE

JAMHURI YA KENYA
REPUBLIC OF KENYA
SERIAL NUMBER 000000000
ID NUMBER 33332222
FULL NAMES
JANE DOE
DATE OF BIRTH
19. 01. 1999
SEX
FEMALE
DISTRICT OF BIRTH
WESTLANDS
PLACE OF ISSUE
KIBERA
DATE OF ISSUE
11. 01. 2011
HOLDER'S SIGN

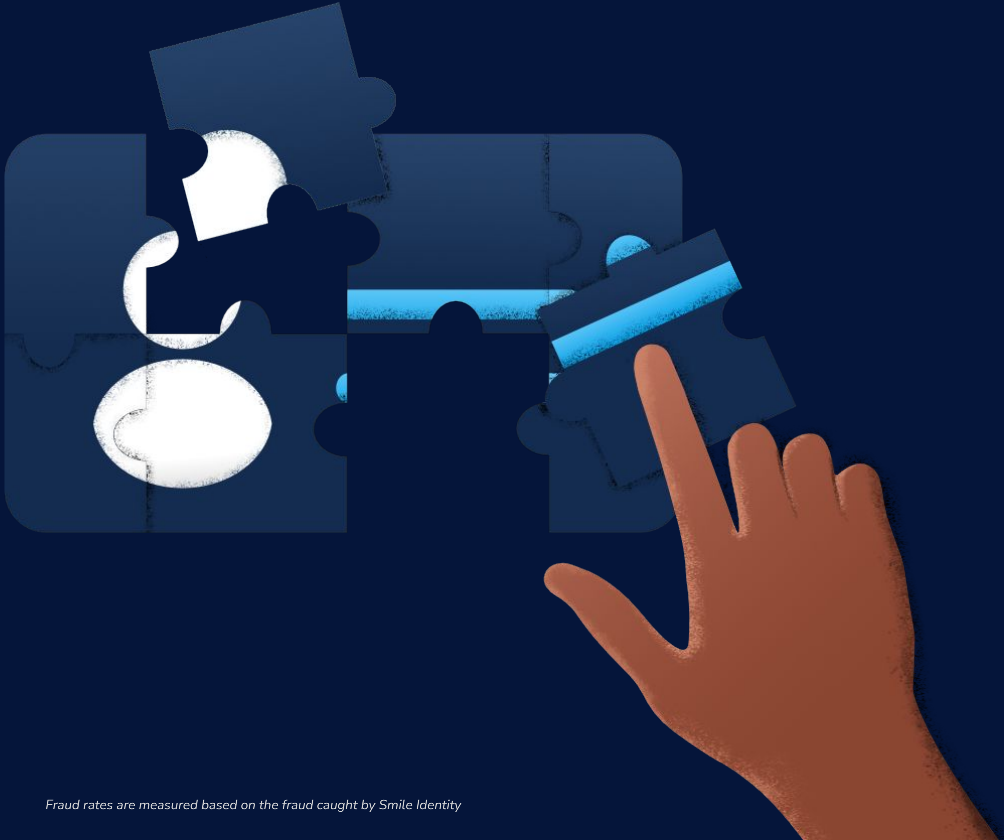


Compliance Rules for Data Access

In 2019, Kenya introduced the Data Protection Act. It is the main regulation governing the collection and processing of personal data in Kenya. This act requires user consent for processing the personal data of Kenyans and aliens living in Kenya.

In addition, the Act requires any business collecting personal information to register as a data controller and anyone processing data to be a registered processor. Smile Identity has an existing memorandum of understanding (MoU) with the Kenyan government to verify the National ID for KYC.

Sources: CIA World Factbook Kenya, World Bank ID4D Global Findex Survey



The challenges of consolidating data across an entire country

The biggest opportunity for biometric verification is the consolidation of data

The Kenyan National ID database is missing photos for roughly 40% of registered persons. When the photo is missing from the database, Smile Identity reverts to matching to an ID document however, many Kenyans don't carry their original ID document but rather a photocopy. This makes verifying ID documents a challenge in Kenya.

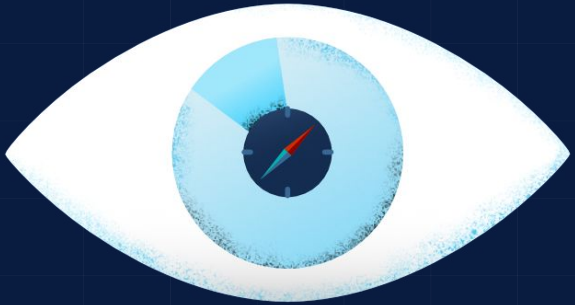
Kenya held an exercise in 2019 to register all citizens for a new system known as "huduma namba." This new biometric ID document combines all identity information from government agencies, such as the National ID, health insurance, and tax number, into one.

In 2021, it was put on hold after the High Court of Kenya ruled that data collection and processing did not follow the Data Protection Act and that a data protection impact assessment (dpia) must be conducted prior to processing of data and the roll out of the Huduma Cards. Kenyans currently await the outcome of the dpia, which may enable the roll out of huduma namba.

Fraud rates are measured based on the fraud caught by Smile Identity

Types of Fraud Attacks

Fraud methods we frequently encounter



Fraud comes in many shapes and sizes

As technology advances, the techniques that fraudsters use are also evolving. Passwords and authentication codes are becoming less common as more providers are moving towards the more secure biometrics solutions. But, fraudsters aren't far behind, and they've got a few tricks up their sleeves to fool security systems.

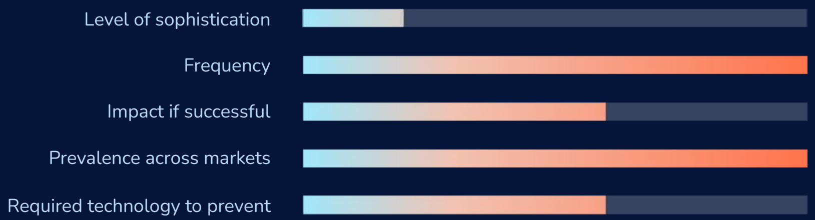
Here are some of the tactics we see fraudsters attempting today.

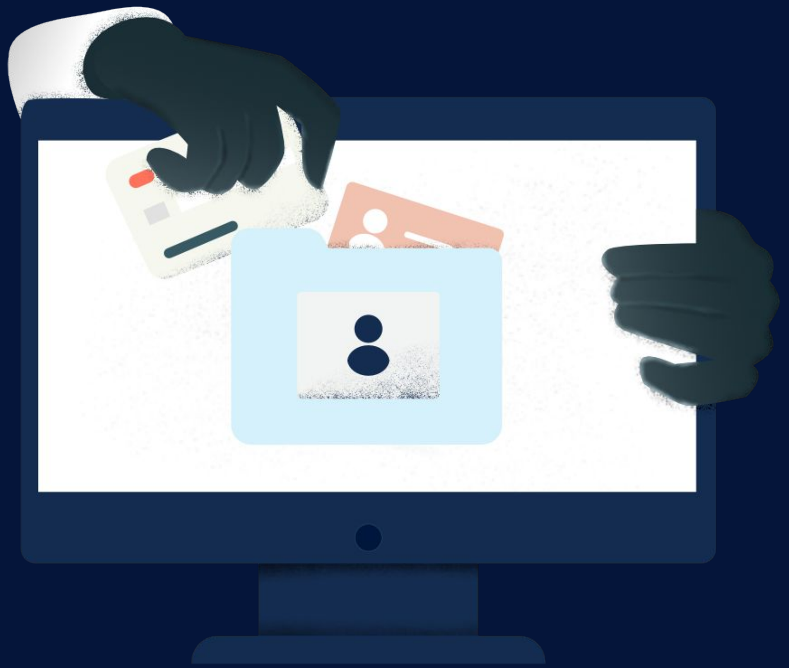
Stolen ID Information

The most common fraud attempts we see are stolen IDs. This is when a user tries to sign up to a service using an ID number or document that is not their own.

Since these IDs are genuinely authentic, they may pass a basic KYC check. However, these fraud attacks are easily blocked by Smile Identity's **Biometric KYC**. Comparing user submitted selfies to an official ID photo or document reveals whether the person behind the screen is the ID owner.

A key pillar to identity verification is not only confirming whether an ID number or document is valid and authentic but also that it's being used by the rightful owner.





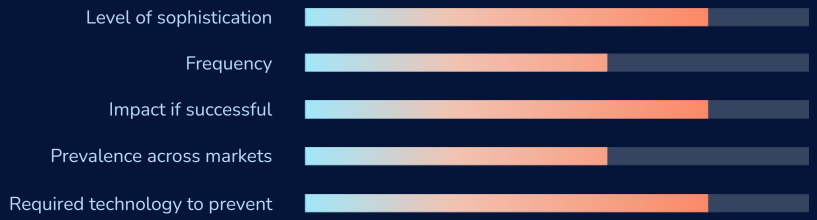
Of all the biometric fraud attempts Smile Identity caught in the first half of 2022, 48% were cases where an ID was valid but the face did not match the ID owner.

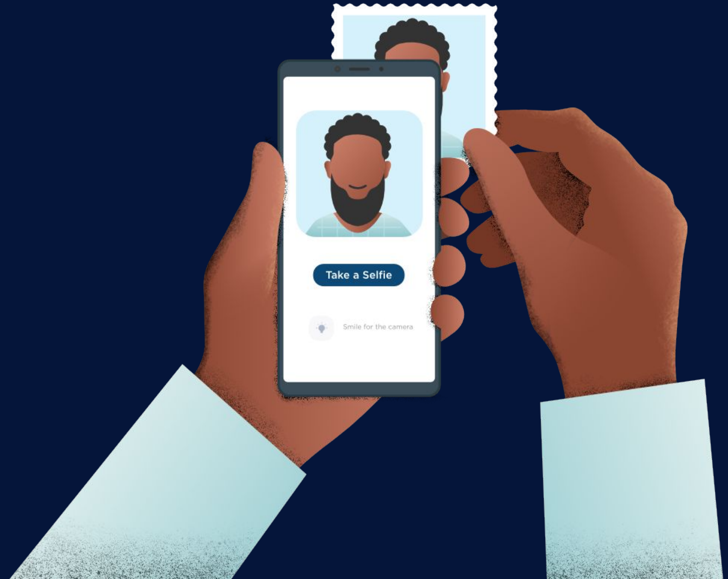
Selfie Spoofs

Our systems have detected some sophisticated fraud attempts, such as spoofing attacks. A selfie spoof is when someone tries to forge the presence of an authentic user with a photo. Some examples of this are: photos of prints, photo from a device, and printed face masks. These are sometimes referred to as “cheapfakes”.

Occasionally, these are benign mistakes where the user didn't follow or understand the instructions and instead presented a photo from their device. However, more often than not, it indicates that a fraudster is attempting to present themselves as someone else. The majority of the time, fraudsters obtain social media images or videos of the people they wish to impersonate.

At Smile Identity, we perform motion liveness checks to ensure that the person behind the camera is the original user. Some fraudsters who are aware of liveness technology may attempt to dupe the system by presenting a video saved on their device. This is called a “replay attack.”





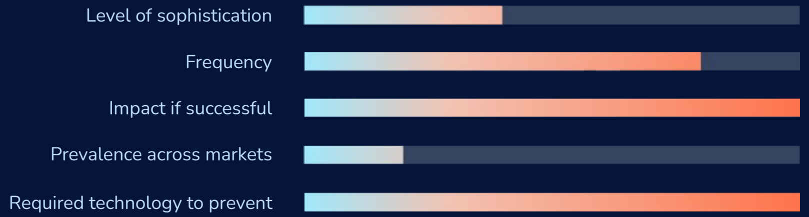
Duplicate Accounts

Most businesses run promotions to reward existing clients or attract new sign ups. We have noticed that this makes them vulnerable to a new kind of fraud known as "duplication fraud". Fraudsters will sign up multiple times so that they can collect the rewards many times over.

There are two common methods of duplication fraud:

- **Serial Submitters:** These individuals will try to gain access by submitting the same ID information as many times as possible. As rampant as this type of fraud can be, it is heavily reliant on the resilience of the fraudster and can be mitigated by sign-up caps or checks against previously used ID numbers.

- **Database Infiltrators:** These individuals have found ways to access ID authority databases and pose a much greater threat. With this access, they are able to create seemingly legitimate identities by registering multiple times with an ID authority. These identities will appear valid during a basic government database check even with face match. This fraud can only be caught using ***biometric de-duplication.***



Synthetic Fraud & Deepfakes

What is synthetic fraud?

Synthetic identity fraud combines legitimate and fake information to create a new fake persona. Because some of the information is legitimate, it can be more difficult to catch. When a fraudster uses this method, they can remain undetected for an extended period of time if subsequent checks using additional information are not done.

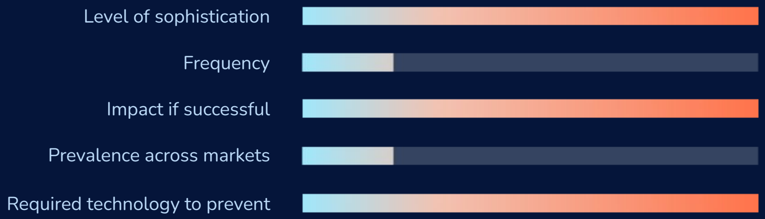
Random face generators are an emerging type of synthetic fraud whereby fraudsters use widely available computer vision algorithms to create faces that look like real people but are entirely fictitious. **These attacks can be mitigated by checking against National Databases using Smile Identity's Biometric KYC.**

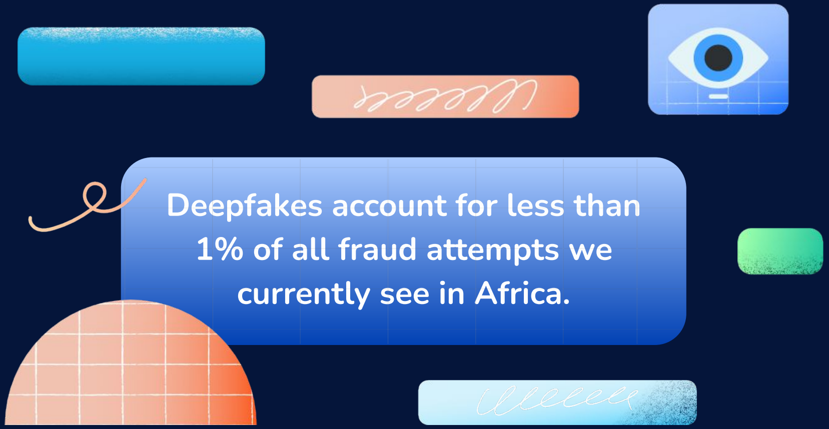
Deepfakes are not a major threat... yet.

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 are used to make it seem like the target did or said something that they, in fact, did not.

This is typically done by superimposing face images of actual people on to videos or three dimensional computer vision models.

The techniques required to produce high quality deepfakes at scale are still beyond the reach of most fraudsters and they tend to look for easier ways in.

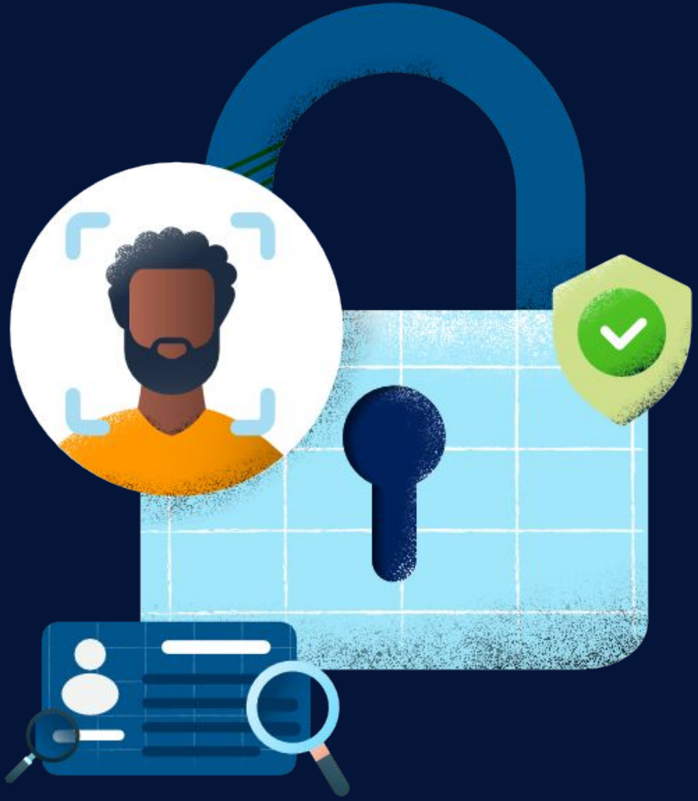




Deepfakes account for less than 1% of all fraud attempts we currently see in Africa.

Prevention

How Smile Identity can help you prevent fraud



Biometric KYC: The key to fraud prevention

Verifying ID numbers alone is insufficient to catch most fraud. Criminals have discovered ways of creating or accessing legitimate ID numbers that will easily pass a textual only ID verification.

Many digital services are turning to biometric face checks to power safe remote onboarding.

These checks match consumers' selfies against IDs or previously enrolled photos to ensure that only legitimate users are signing up for accounts or accessing services online. At Smile Identity, we have witnessed this growth.

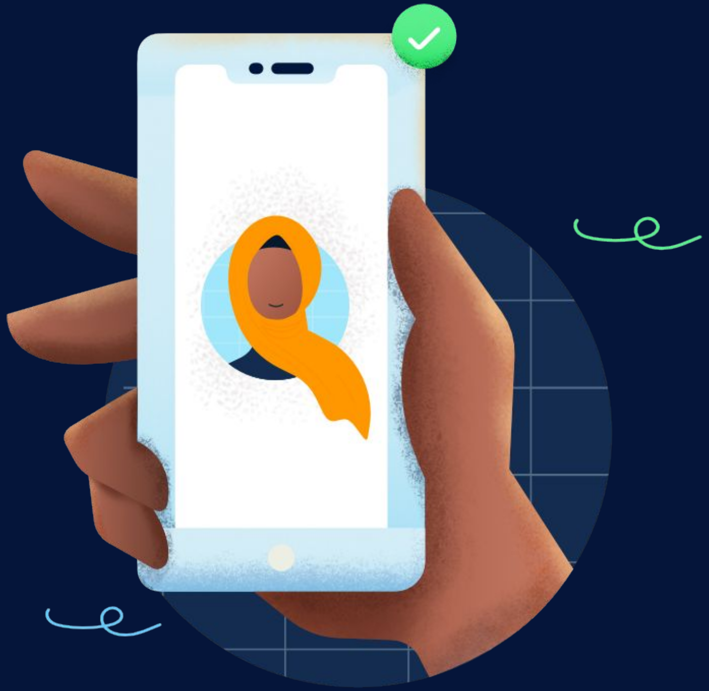
Over the past two years, usage of our Biometric KYC products has increased by 400%.

Biometric solutions are the way forward not only for security but also for user convenience. The rise of selfies in the mid 2010's and the subsequent use of facial biometrics for device access has made consumers more familiar with facial recognition as a medium.

Face verification is more secure and less error prone than manually entering passwords or text.

Smile Identity's Biometric KYC solution matches a user-submitted selfie to the photo on file at an ID authority.

This gives you the confidence of both a reliable database check and a biometric comparison to ensure your users are in fact who they say they are.



Liveness checks are a crucial verification step

Matching faces is not enough.

Biometric checks should be backed up by a strong anti-spoof system to ensure customer safety. While sophisticated attacks like “deepfakes” are still relatively uncommon, so called “cheapfakes” are prevalent. These include taking photos of screens, uploading static photos, or wearing masks.

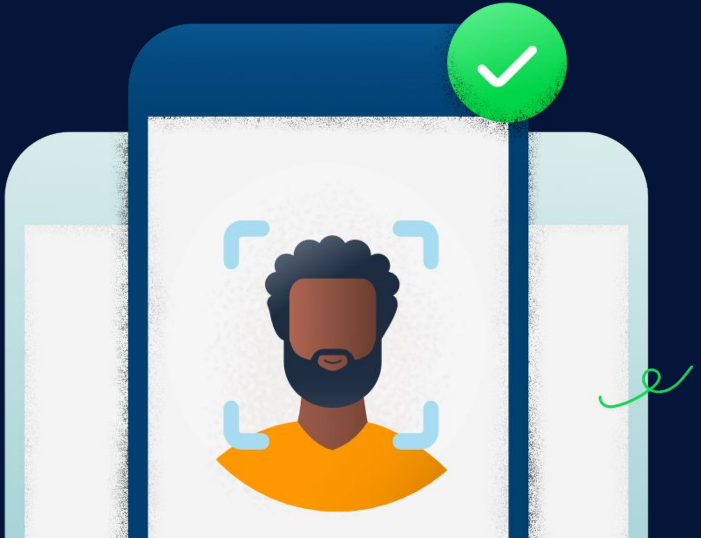
These types of fakes can easily be prevented with a liveness check. Liveness algorithms complement and augment face recognition, resulting in robust KYC that users and app developers can trust.

So, how do these algorithms work?

Many apps that leverage liveness detection capture a short video of the user during registration.

Alternatively, some apps grab a quick succession of shots while the user performs a specific motion or gesture in front of the camera. The liveness detection algorithm processes the image or video with specialized computer vision algorithms, acquiring mathematical confidence that the intended real human was present during image capture.

At Smile Identity, we have been working on face recognition and liveness check solutions since 2016. Our trademarked liveness check technology, SmartSelfie™ , is powered by 6 AI-based anti-spoof models. SmartSelfie™ ensures that fraudsters can’t pass a KYC check with spoof images or videos of faces.



Deduplication prevents users from creating multiple accounts

When fraudsters create multiple accounts to collect promotional payouts or loans, this is known as a duplicate attack. These efforts are only fruitful for fraudsters if they can successfully sign up for many accounts.

While fraudsters have found ways to infiltrate ID systems and have multiple ID numbers, a more difficult thing to alter is their face.

Once we establish the person is real and not a spoof, we run our in-house models to deduplicate their identity. This ensures that the person is only who they say they are and are not signing up under multiple, fake identities.

Deduplication is an extremely powerful tool to prevent duplicate account fraud.

In practice, deduplication searches a history of faces that have been previously verified and alerts you if the same person 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 organized attacks on promotional signup codes.

Smile Secure is a new offering from Smile Identity that helps you prevent users from creating multiple accounts (duplication fraud). It scans previously registered faces in real-time to notify you if a user has signed up for your service in the past, regardless of ID type.

Smile Secure Case Study

Period: January until July 2022
Data: 7 selected partners who ran promotions during period
KYC records analyzed: 1.3 million

The chart below visualizes our findings from running our Smile Secure face deduplication algorithms against millions of past records of selected partners between January and July 2022.

Our observations show two crucial trends across all these partners:

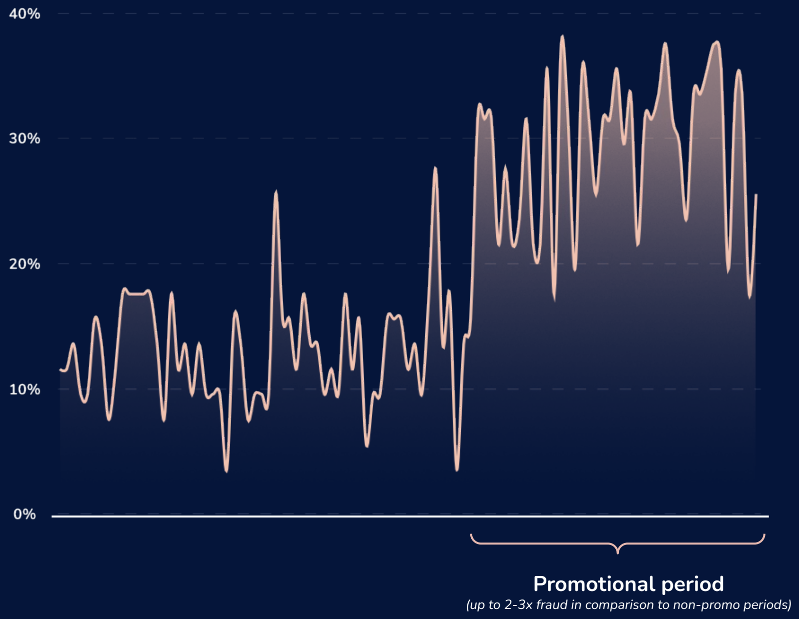
1. A considerable amount of duplicate KYC attempts, (some of which maybe be legitimate if a user cannot retrieve their past account).
2. The percentage of fraud can jump up to 2-3 times during a promotional period, as more fraudsters are attracted.

Most duplications are typically caused by a small percentage of users. However, when deduplication is not used, fraud can reach double digits.

Biometric KYC backed by Smile Secure is the best way to protect your organization against professional fraudsters who are attempting to exploit national databases by registering multiple identities.

% of All KYC Checks by Repeated Users

Recognized by Smile Secure's identity matching against past records

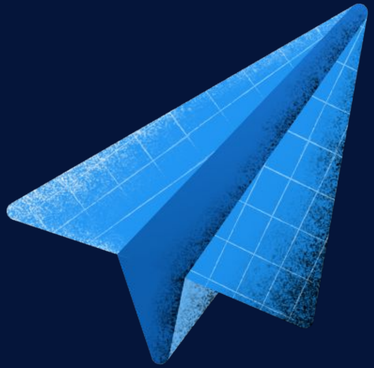


Data and time periods have been anonymized and aggregated. The chart is meant for visualization purposes only but is based on real partner data from a period of January-July 2022. The Smile Secure face matching algorithm has been run against over 8 million KYC records.

Contact Us

Want to learn more about the latest KYC trends across Africa?

Contact us at info@smileidentity.com.



Contributors

Megan
Keirstead
Product Marketing Manager

Lameck
Orina
Graphic Designer and Illustrator

Navid
Scheybani
Chief Growth Officer

Mark
Straub
Chief Executive Officer

Rachael
Wambua
Content and Channel Engagement Specialist

George
Williams
Head of Artificial Intelligence / Human Intelligence