Smile ID

2024 Digital Identity
Fraud in Africa Report

Trends, tactics and solutions needed to tackle fraud effectively.

usesmileid.com

Contents

Foreword

This year, we decided to shift the focus of our annual report from KYC to fraud. We made this decision because as we engaged with customers and observed changes in behaviour over 2023, we saw that an increasing portion of company resources previously allocated to new account creation has shifted to driving consumer engagement and account profitability. Similarly, we have seen a shift in the activities of fraudsters, from exploiting opportunities around new account creation to increasing attempts at account takeover and theft.

So, leveraging our unique dataset covering over 100 million identity verifications on the continent, this year's report focuses on fraud – its methodologies, characteristics and impact across Africa. We follow it with a guide to implementing a comprehensive anti-fraud system to protect your organisation and users. Finally, we end with a future outlook on AI and machine learning and its increasing role in digital identity verification.

This report is the first analysis focused on fraud trends, tactics, and defences across Africa. It will provide decision-makers in Africa with an in-depth look at everything they need to know about mitigating fraud losses for their businesses.

100M Identity Checks in Africa

Identity fraud is a growing problem across Africa, costing businesses millions each year. As more financial transactions and commerce move online, verification of individuals' identities is paramount to reduce deception and criminal activities.

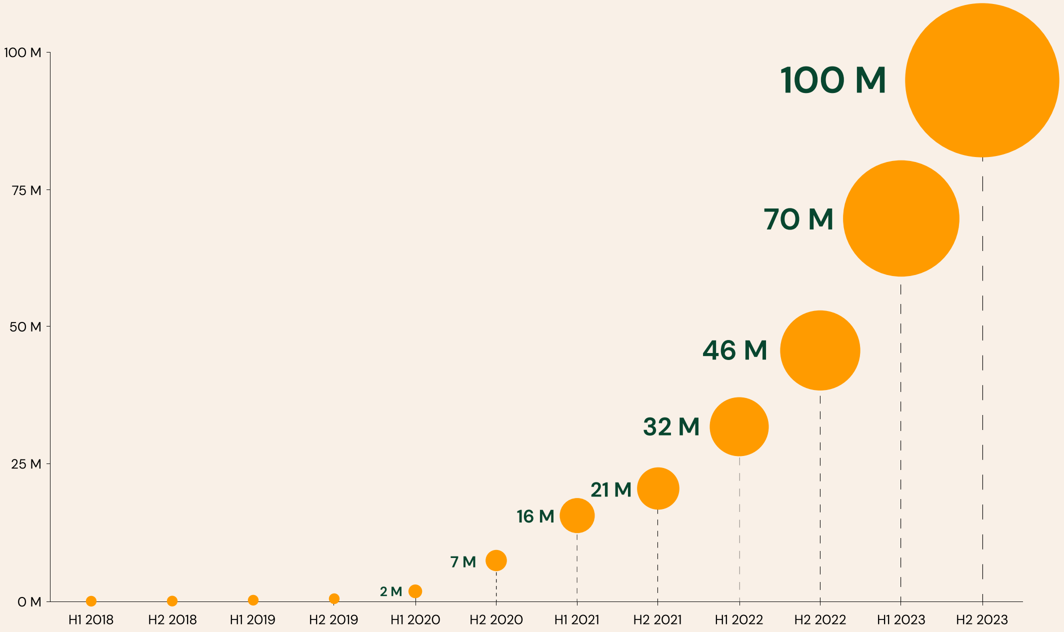
With over 100 million identity checks conducted to date - more than any other provider in Africa - Smile ID has firmly established itself as the continent's leader in identity verification. By combining world-class technology with pan-African local presence, we play a crucial role in the fight against identity fraud.

Not only does identity verification help businesses meet legal requirements, it is also a key defense mechanism, as customers who undergo the process are statistically less likely to engage in fraudulent activities.

As the leading ID verification provider in Africa, we have helped onboard tens of millions of valuable users for our customers, while reducing fictitious signups by as much as 90%.

In the following pages, as we break down fraud data and trends across Africa, we will also spotlight different identity verification solutions you can leverage to tackle fraud while maintaining a smooth user experience.

Total verifications completed from 2018 to date



Note on chart and dataset: This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from all verifications completed by Smile ID from 2018 to Dec 2023.

Key Takeaways

4X

Biometrics detect 4x more fraud

Businesses that rely on textual verification alone are four times more likely to be defrauded than their counterparts that use biometrics.

13%

Biometric fraud rate reached 13%

Fraudsters are evolving their tactics. Q4 2023 saw a record high 13% of biometric verification attempts marked as fraudulent.

80% of fraud attacks focused on National IDs

80% of fraud attacks on the continent are concentrated on national ID cards, making them Africa's most attacked document type.

Percentage of Women now 35% of all verifications

Gender inclusion is rising across all African regions as % of women verified has increased from 10% in 2019 to 35% in 2023.

Multi-factor authentication is needed to curb transaction fraud

Transaction fraud is rising, necessitating multi-factor authentication across the entire customer lifecycle.

SDKs result in higher performance

Compared to APIs, SDKs are better suited for ID verification in Africa because they can be engineered with regional considerations in mind.

Active liveness responsible for 87% of biometric fraud caught

87% of biometric fraud caught is due to active liveness checks showing that selfies alone are insufficient.

Payments fraud spiked past 40%

The payments industry suffered significant levels of fraud in 2023 with fraudulent verification attempts reaching as much as 42% in February and 35% in August.

Data Analysis

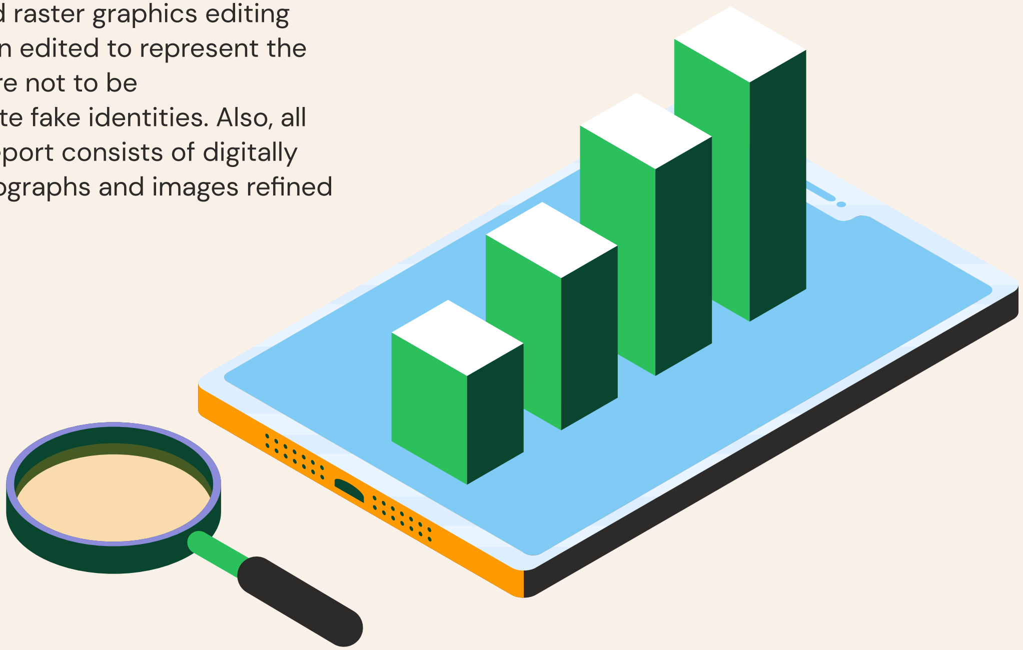
This report uses anonymised data collected from identity verification attempts in Smile ID systems. It is our best effort to reflect trends on the African continent based on verifications conducted in our systems.

The data in our systems cuts across textual, biometric, and document verifications. Although fraud can be observed in all three types, this report focuses on biometric and document fraud. We observe more sophisticated attacks during biometric verifications than when verifying textual information alone, warranting a deeper dive into methods and tactics.

This report's analysis and estimation methods include a combination of random sampling, statistical modelling, and descriptive analysis directly from verifications in Smile's systems.

Imagery

ID documents in this report have been digitally created using vector and raster graphics editing software. They have been edited to represent the actual documents but are not to be misappropriated to create fake identities. Also, all human imagery in this report consists of digitally manipulated stock photographs and images refined with the help of AI.



01

Methodology of Fraud

In this section, we examine the evolving tactics used by fraudsters in the digital age, drawing from the latest trends, case studies, and expert insights. We aim to demystify the advanced techniques of fraud, offering insights into fraudster behaviour and how businesses can counteract these threats to bolster their defences against digital fraud.

Document Fraud

Government-issued ID documents remain the cornerstone for ID verification in today's digital world. In most regions, businesses, especially financial institutions, must collect and verify ID documents during onboarding to regulate access to their services. Fraudsters seeking to access financial services will usually attempt to bypass onboarding protocols using compromised documents.

Document fraud involves misrepresenting an ID document to mislead others about the holder's identity. While the exact methodologies of document fraud might differ, they generally fall into two broad categories:

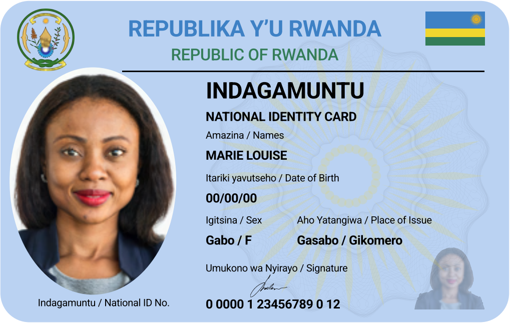
- **Fake Documents**
- **Stolen IDs**

1. Fake Documents

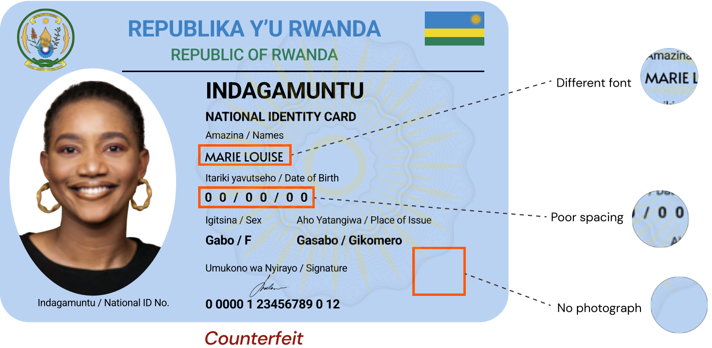
These are forged or falsified identification materials that individuals use to misrepresent their identity. Typically, these documents mimic authentic ID documents. Most fake ID document attempts are poorly done and can be filtered out by an eye test. Three types of document fraud include:

a. Counterfeit Document:

This is typically a forgery of an original ID document. Usually, counterfeit documents will lack some or all of the security features on an original ID, e.g. holographs, watermarks, biometrics, etc. They also contain obvious errors like different fonts, poor spacing, colour, missing design elements, etc. This kind of fraud can be caught by comparing the document to an authentic template.



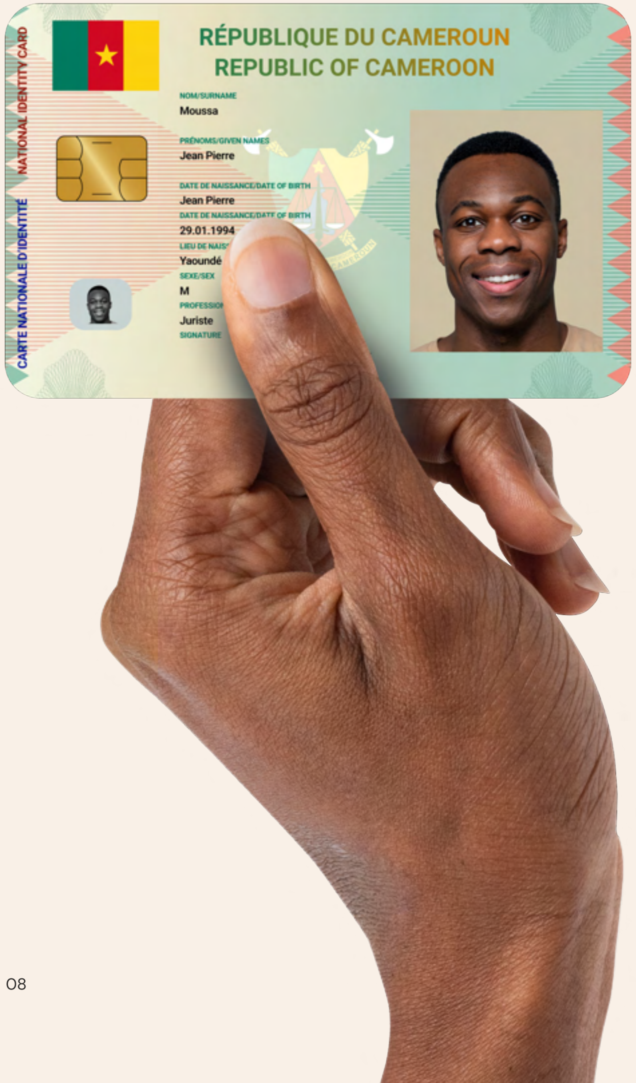
Original



Counterfeit

b. Obscured Document:

Some fraudsters may obscure details on ID documents to make them unreadable. This typically happens when they use their original ID documents, as exposing their real identities puts them at risk.



CARTE NATIONALE D'IDENTITÉ NATIONAL IDENTITY CARD

RÉPUBLIQUE DU CAMEROUN
REPUBLIC OF CAMEROON

NOM/SURNAME
Moussa

PRÉNOMS/GIVEN NAMES
Jean Pierre

DATE DE NAISSANCE/DATE OF BIRTH
Jean Pierre

DATE DE NAISSANCE/DATE OF BIRTH
29.01.1994

LIEU DE NAIS
Yaoundé

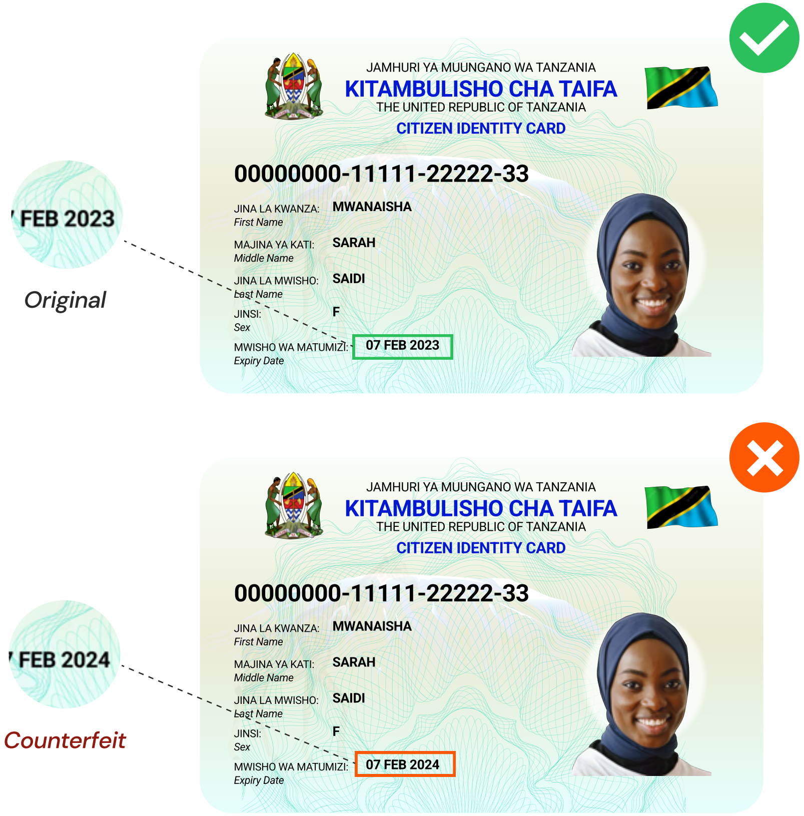
SEXE/SEX
M

PROFESSION
Juriste

SIGNATURE

c. Expired Document:

Most ID cards expire and require renewal. Fraudsters can steal people's identities using expired ID documents if not properly disposed of.


FEB 2023
Original
FEB 2024
Counterfeit

JAMHURI YA MUUNGANO WA TANZANIA
KITAMBULISHO CHA TAIFA
THE UNITED REPUBLIC OF TANZANIA
CITIZEN IDENTITY CARD

00000000-11111-22222-33

JINA LA KWANZA: *First Name* MWANAISHA
MAJINA YA KATI: *Middle Name* SARAH
JINA LA MWISHO: *Last Name* SAIDI
JINSI: *Sex* F
MWISHO WA MATUMIZI: *Expiry Date* 07 FEB 2023

JAMHURI YA MUUNGANO WA TANZANIA
KITAMBULISHO CHA TAIFA
THE UNITED REPUBLIC OF TANZANIA
CITIZEN IDENTITY CARD

00000000-11111-22222-33

JINA LA KWANZA: *First Name* MWANAISHA
MAJINA YA KATI: *Middle Name* SARAH
JINA LA MWISHO: *Last Name* SAIDI
JINSI: *Sex* F
MWISHO WA MATUMIZI: *Expiry Date* 07 FEB 2024

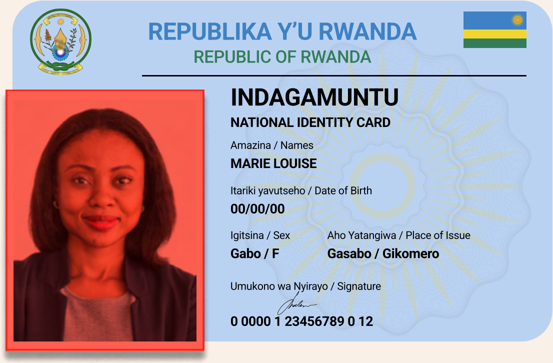
Note: Using expired IDs does not always indicate fraud; factors like regional conflicts, natural disasters, or lack of renewal policies may prevent timely updates. Rejecting expired IDs should be done on a case-by-case basis.

2. Stolen IDs

Faking ID documents to a realistic level requires more skill than most fraudsters have. Most document fraud attempts come from real but illegally obtained documents. With Government IDs becoming mandatory and ubiquitous in most countries, fraudsters have many ways to access stolen documents.

Common ways that fraudsters get access to real documents include when they get lost at festivals, concerts, markets or pickpocketed from wallets. Scammers can also buy stolen ID information on the dark web from database hacks that are common across the region. Since 2017, data hacks have been reported in multiple African countries, including Nigeria, Ghana, South Africa, and Egypt.

Fraudsters commonly use stolen IDs by altering parts of a document to change information about its ownership.



REPUBLIKA Y'U RWANDA
REPUBLIC OF RWANDA

INDAGAMUNTU
NATIONAL IDENTITY CARD

Amazina / Names
MARIE LOUISE

Itariki yavutseho / Date of Birth
00/00/00

Igitsina / Sex
Gabo / F

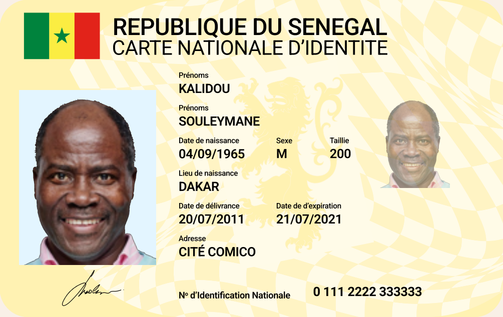
Aho Yatangiwa / Place of Issue
Gasabo / Gikomero

Umukono wa Nyirayo / Signature

0 0000 1 23456789 0 12

ID with an obviously replaced picture of the holder

Another way fraudsters are using stolen IDs is to upload a picture of a picture of an ID document during ID verification.



REPUBLIQUE DU SENEGAL
CARTE NATIONALE D'IDENTITE

Prénoms
KALIDOU

Prénoms
SOULEYMANE

Date de naissance
04/09/1965

Sexe
M

Taillie
200

Lieu de naissance
DAKAR

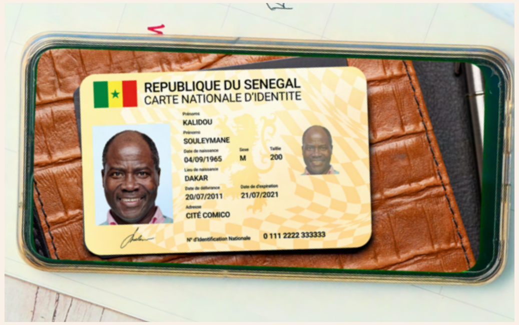
Date de délivrance
20/07/2011

Date de d'expiration
21/07/2021

Adresse
CITÉ COMICO

Nº d'Identification Nationale 0 111 2222 333333

Original



REPUBLIQUE DU SENEGAL
CARTE NATIONALE D'IDENTITE

Prénoms
KALIDOU

Prénoms
SOULEYMANE

Date de naissance
04/09/1965

Sexe
M

Taillie
200

Lieu de naissance
DAKAR

Date de délivrance
20/07/2011

Date de d'expiration
21/07/2021

Adresse
CITÉ COMICO

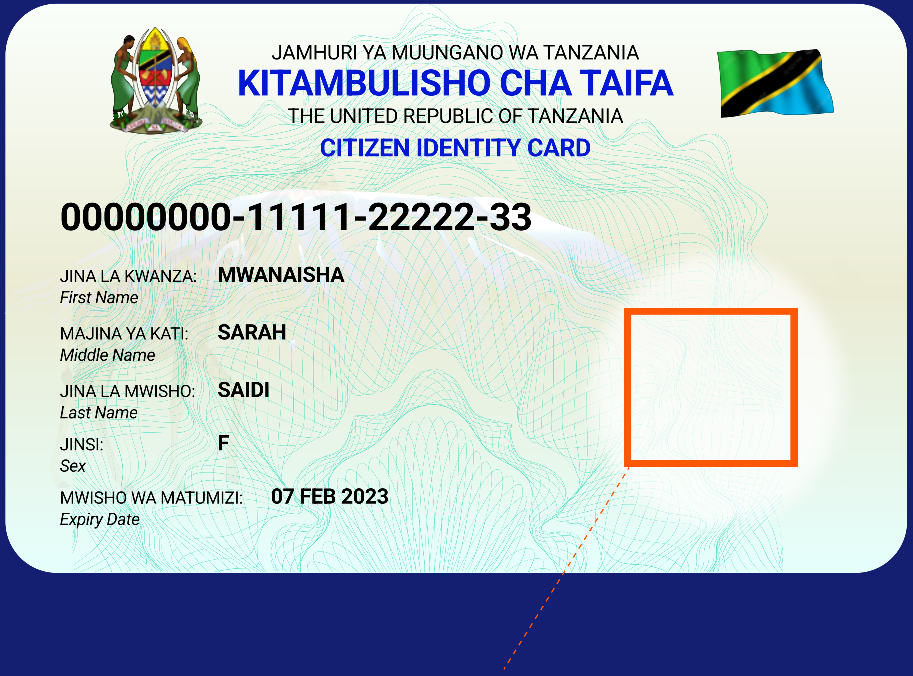
Nº d'Identification Nationale 0 111 2222 333333

Picture of picture

ID documents without biometric information are most vulnerable to stolen ID attacks.

Where available, Biometric verification solutions provide an extra layer of protection against stolen ID fraud.

At Smile ID, we have different biometric solutions that compare user-submitted selfies to either the photo of the user on file in an ID authority database, or the photo on the document, ensuring that the person interacting with a service is the legitimate ID holder. This critical component of identity verification extends beyond merely validating the legitimacy and authenticity of an ID document.



JAMHURI YA MUUNGANO WA TANZANIA
KITAMBULISHO CHA TAIFA
THE UNITED REPUBLIC OF TANZANIA
CITIZEN IDENTITY CARD

00000000-11111-22222-33

JINA LA KWANZA: *First Name* MWANAISHA

MAJINA YA KATI: *Middle Name* SARAH

JINA LA MWISHO: *Last Name* SAIDI

JINSI: *Sex* F

MWISHO WA MATUMIZI: *Expiry Date* 07 FEB 2023

Photograph missing on ID

Tackling Document Fraud

There are two common ways that businesses can fight document fraud. Businesses can either verify the ID's validity against ID authority databases or through document verification by comparing the ID document with authentic templates and security features to find inconsistencies.

Since document fraud involves the manipulation of actual documents, bad actors can bypass text-only verification measures that simply validate numbers against a database.

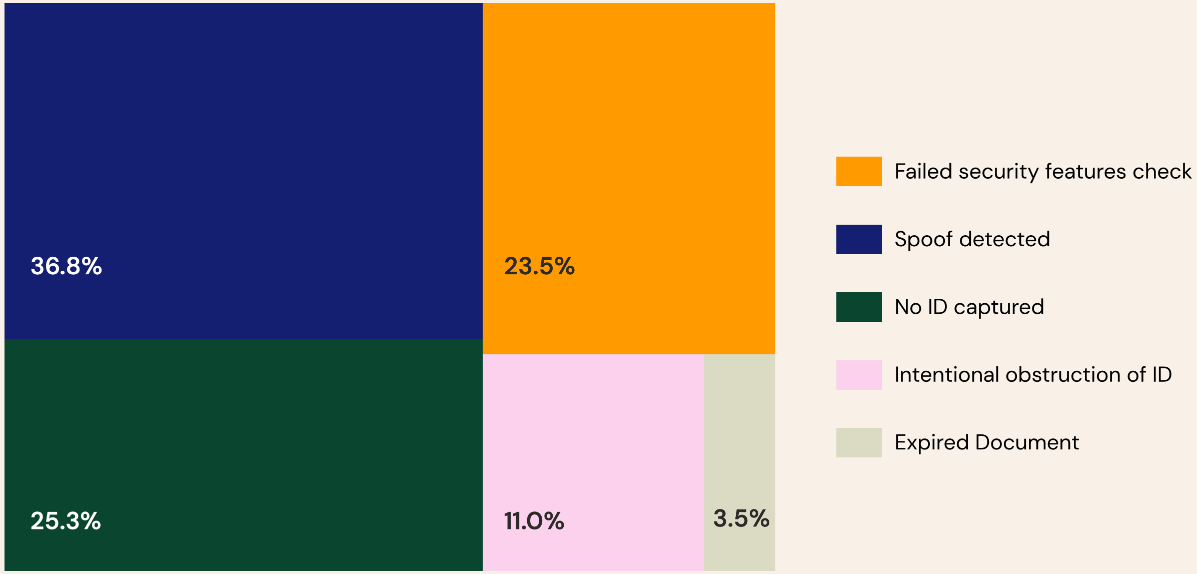
Combining document verification solutions with biometric authentication adds an additional layer of security, ensuring that only authentic documents from real people scale through.

Incidentally, 37% of the fraud performed on documents was caught due to the biometric component in our document verification solution. **Without biometric checks, we estimate more than a third of ID document fraud goes unnoticed.**

However, document ID fraud is not always a failure of ID verification systems. Some ID types, especially those without security (biometric or otherwise) systems, are more prone to attack.

Breakdown of document fraud in Africa

Across all verifications done by Smile ID, below is a breakdown of document fraud attempts per type.



Note on chart and data set:
This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from all verifications completed by Smile ID from 2021 to Dec 2023. Fraud analysis in this chart excludes the submission of invalid and poor-quality images.

Smile ID’s Document Verification

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.

Smile ID also consistently delivers higher pass rates than any other provider in Africa without compromising on speed or security. With an average pass rate of 80% across Africa, we help you to convert good users fast.

Effectively tackle document fraud by using either of our two document verification solutions:

Document Verification	Enhanced Document Verification
Our document verification product lets you verify the authenticity and ownership of identity documents by comparing the user's selfie to the photo on the document.	Enhanced Document Verification combines all the features of our document verification product with a cross-check against government database in a single call.
Features include document authentication, selfie comparison and OCR.	Features include document authentication, selfie comparison, Issuer data cross-check, and OCR.

Contact Us

User Selfie

ID Authority Photo

ID Authority Response

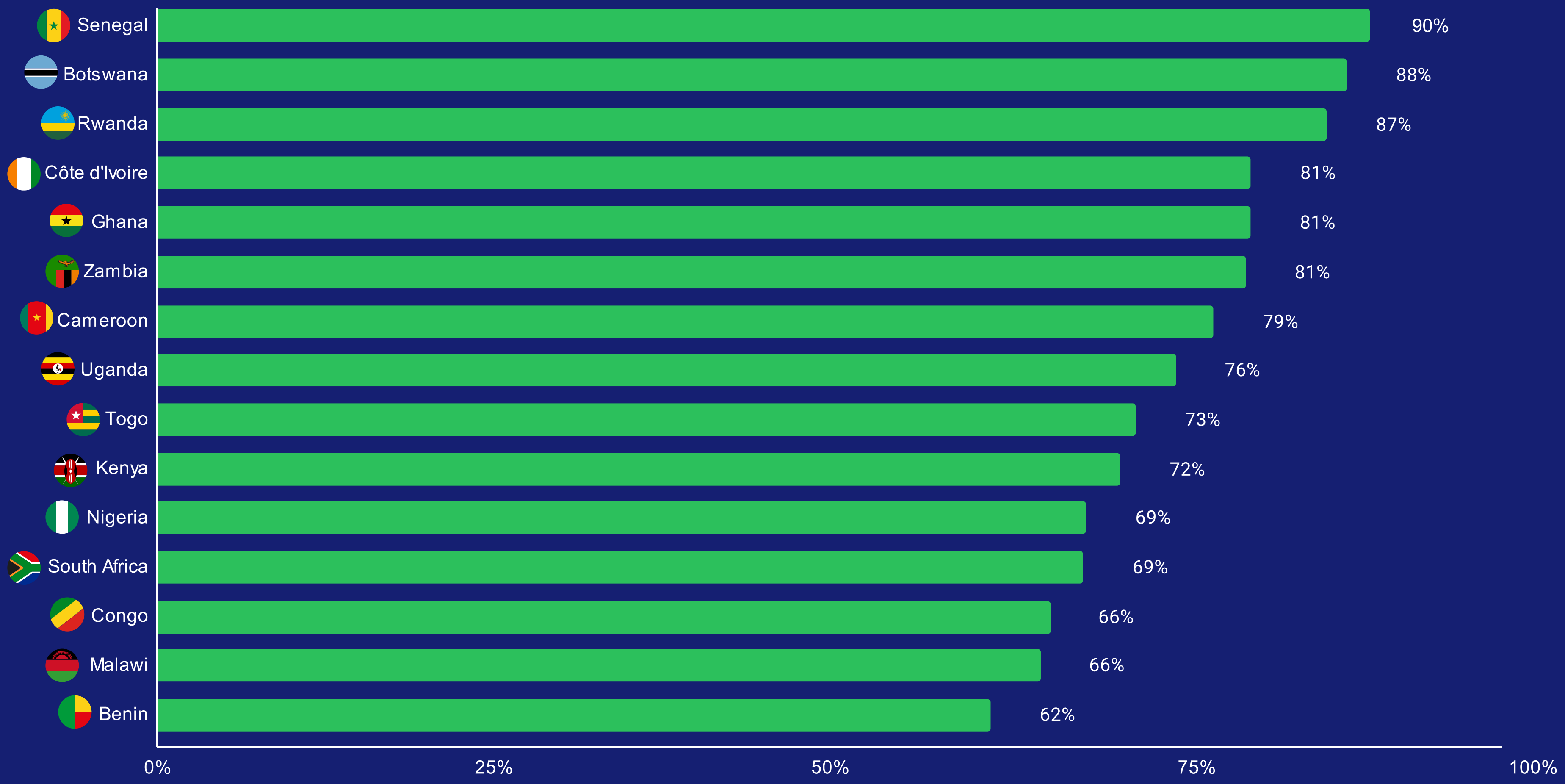
User Provided Info

Type	Detail
Provider	Nimc
ID Type	NIN
ID Number	9484848484
Date of Birth	04/09/1991
Expiry Date	18/02/2020

Accurately verify customers anywhere

- ☑ Technical integration options for every device and OS combination.
- ☑ No Code solution for businesses to build a custom verification web. application and share with end-users through a secure link.
- ☑ 3 or more ID types covered for all African markets.
- ☑ 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%.

Top 15 Countries by Smile ID document Verification Pass Rates



Note on chart and data set: This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from all verifications completed by Smile ID from 2021 to Dec 2023. Fraud analysis in this chart excludes the submission of invalid and poor-quality images.

Smile ID X Bridgecard

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

Goal

Pan-African regulatory compliance

Use case

Payments / Card Issuance

Countries using Smile

Angola

Benin

Cote D'Ivoire

Cameroon

Rwanda

The Problem

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

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

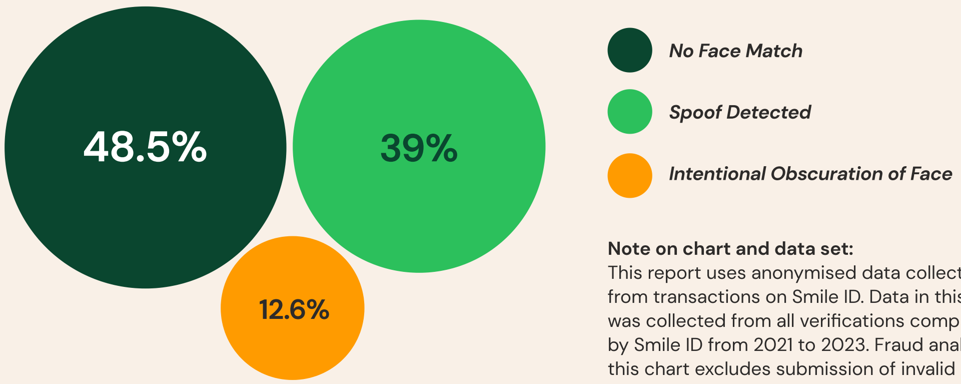
Biometric Fraud

As most African countries move towards stronger ID documents with biometric security; fraudsters are evolving their methodologies. Biometric fraud is usually more complex than document fraud and difficult to catch without advanced prevention tools. It involves the unauthorised and fraudulent use of biometric data such as fingerprints, facial features, iris patterns, or voice for identity verification. It is often performed in tandem with document fraud to trick biometric systems into accepting fraudulent data.

While there are many ways that biometric data can be manipulated for identity fraud, most biometric fraud generally falls into four categories:

1. **No face match**
2. **Spoofing**
3. **Duplication**
4. **Generative AI (Deep fakes)**

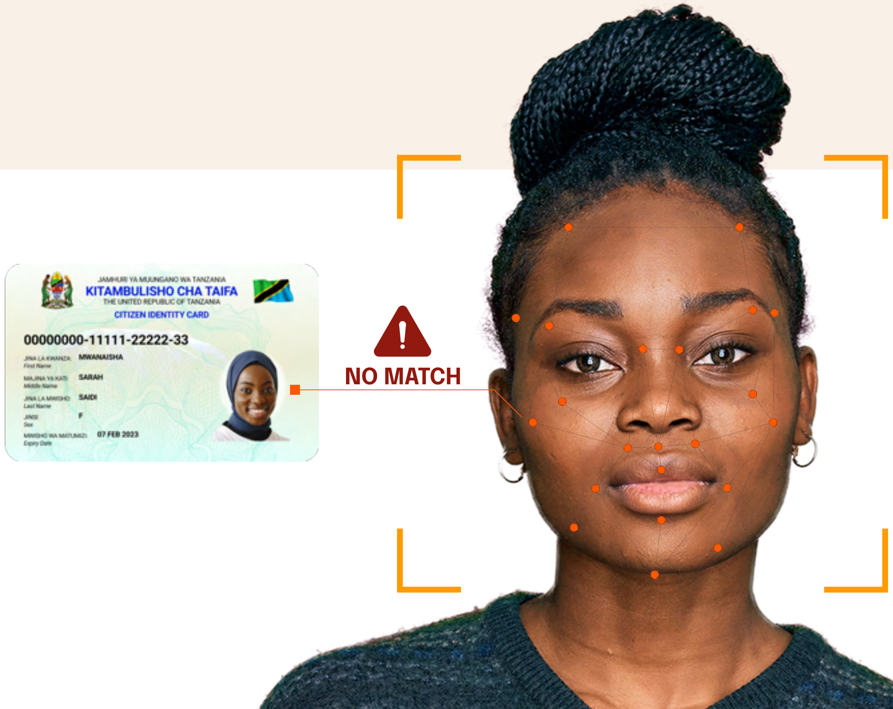
Biometric Fraud in Africa



Note on chart and data set:
This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from all verifications completed by Smile ID from 2021 to 2023. Fraud analysis in this chart excludes submission of invalid and poor quality images.

1. No Face Match

This type of fraud is caught when the selfie submitted by the user doesn't match the face on the ID document or the ID authority image - potentially due to a stolen ID. **No face match accounts for 48.5% of all biometric fraud attacks caught by Smile ID.**


JAMHURI YA MUUNGANO WA TANZANIA
KITAMBULISHO CHA TAIFA
THE UNITED REPUBLIC OF TANZANIA
CITIZEN IDENTITY CARD

00000000-11111-22222-33

JINA LA KWANZA: First Name MWANAISHA
MAJINA YA KATI: Middle Name SARAH
JINA LA MWISHO: Last Name SAIDI
JINSI: Sex F
MWISHO WA MATUMIZI: Expiry Date 07 FEB 2023

2. Spoofing

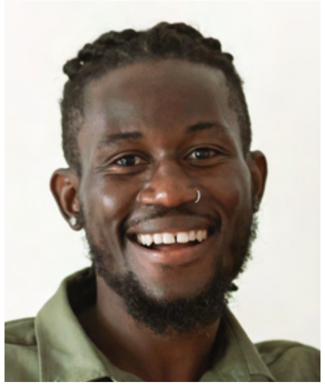
To get around biometric verification systems, fraudsters will sometimes try to mimic the biometric traits of legitimate ID holders. This kind of fraud is commonly referred to as spoofing.

Over the last two years, spoofing attacks were 39% of all biometric fraud attacks caught by Smile ID.

In practice, spoofing attacks may look like the fraudster using a photograph of the ID holder to pass selfie or liveness checks.

Examples of Spoofs

One example we've seen at Smile ID is life-sized printouts of the ID holder's picture.



Submitted image

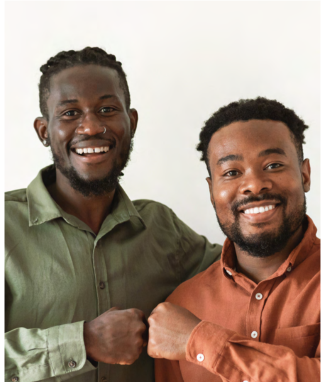
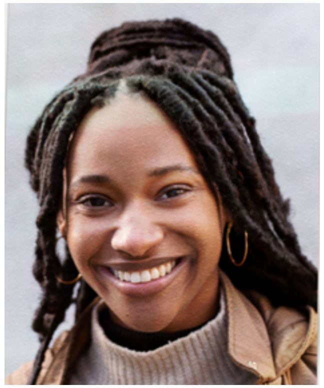


Image shown to be a cutout from a photo

We've also seen this done digitally.



Submitted image

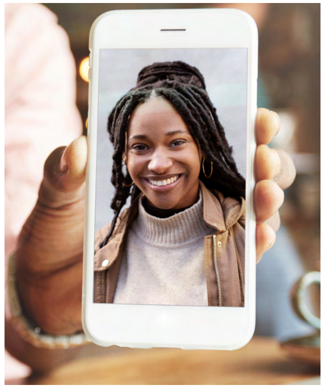


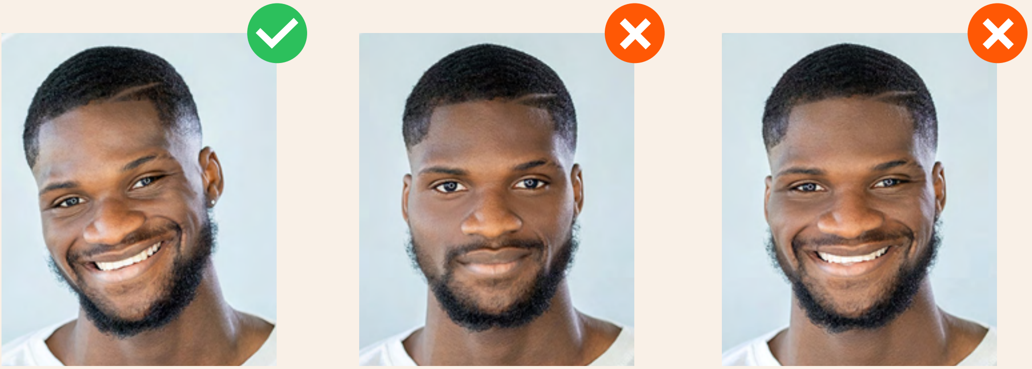
Image shown to be photo on a phone

3. Duplication

Unlike spoofing, which involves a fake representation of a biometric trait, duplication involves using a person’s actual biometric data, sometimes without their consent. Usually, in a duplication attack, the fraudster will try to sign up for a digital service multiple times with the same details to gain some benefit, e.g. signup referral rewards or bonuses. The hallmark of a duplication attack is multiple signups with the same face or ID number.

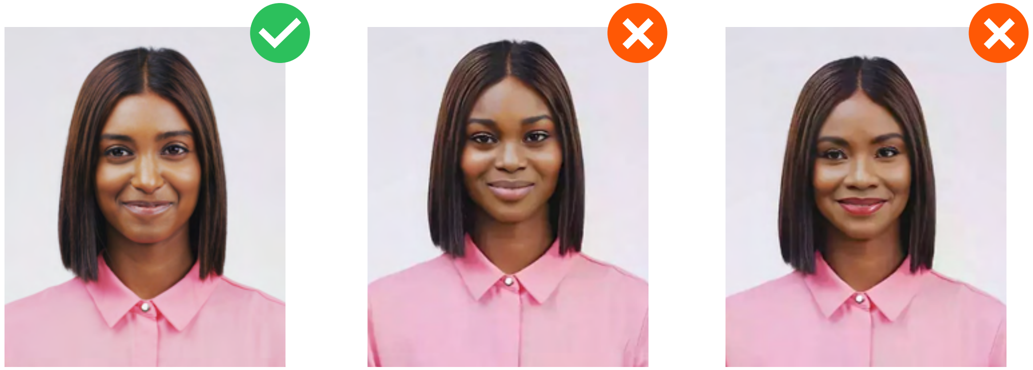
At Smile ID, we have seen over 300 duplicate submissions from a user on a single ID number.

Some fraudulent actors attempt to combine stolen ID documents with duplicated biometric information to beat verification systems.



4. Generative AI (Deep Fakes)

While Generative AI and deepfakes represent a significant advancement in artificial intelligence, they pose new challenges to biometric fraud prevention. Generative AI solutions like Generative Adversarial Networks (GANs) can generate new data similar to the data they were trained on. For businesses looking to prevent fraud, this could mean being inundated with fake IDs, synthetic faces, voices, and other biometric identifiers that are indistinguishable from real ones. Deepfakes can also be used to recreate a person's likeness, including their face and voice, posing a direct threat to biometric authentication systems.



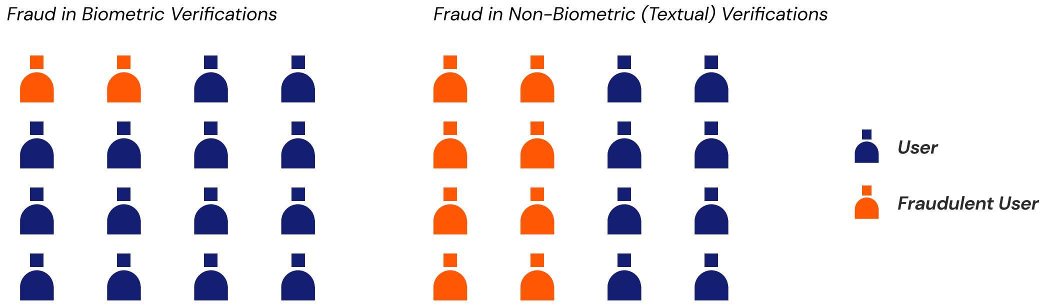
Why Biometrics: Role of Biometric Authentication in Verification

An ideal identity verification system should be capable of verifying that the ID presented is an original issued by the appropriate agency and authenticating that the person presenting the document is the owner.

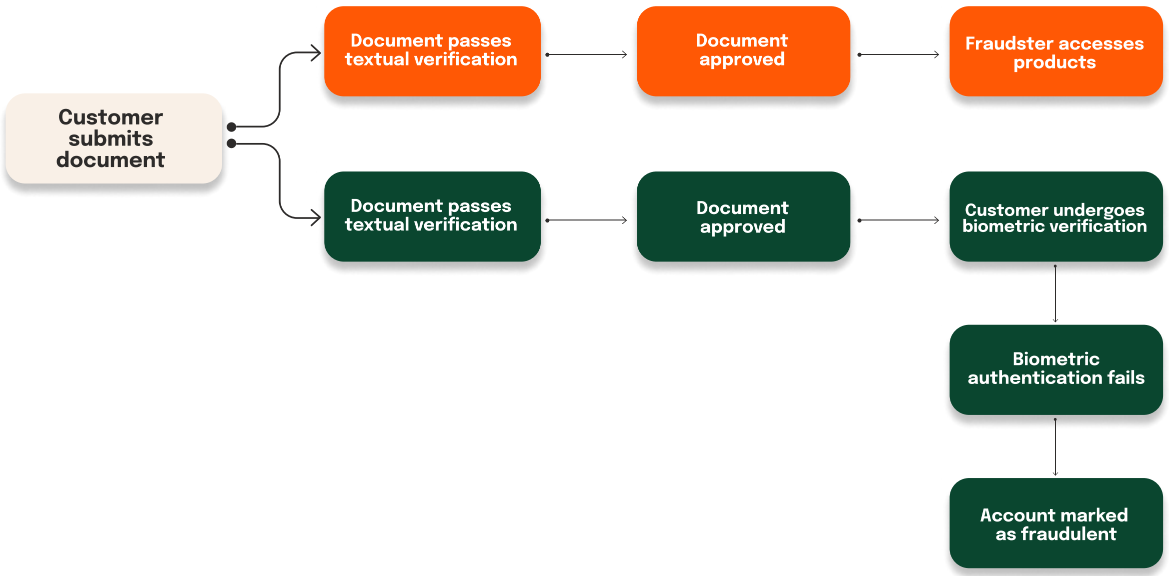
Textual verification solutions that rely on only ID authority access or document authentication are usually capable of verifying the authenticity of a document. However, they cannot authenticate that the person presenting the document is the real owner.

Layering biometric authentication on top of textual verification during onboarding offers advanced protection for businesses. Biometric authentication allows businesses to compare biometric information on the ID document, such as fingerprints, facial features, iris patterns, or voice, with the information collected from the user at the point of authentication.

Smile ID found that businesses that rely on biometric verification are 4 times more safer than their counterparts that rely on textual verification alone.



Note on chart and data set: This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from all verifications completed by Smile ID from 2019 to Dec 2023. Fraud analysis in this chart includes biometric fraud, document fraud, and data validation errors when checking against the government ID database.



Customer submits document

Document passes textual verification → Document approved → Fraudster accesses products

Document passes textual verification → Document approved → Customer undergoes biometric verification → Biometric authentication fails → Account marked as fraudulent

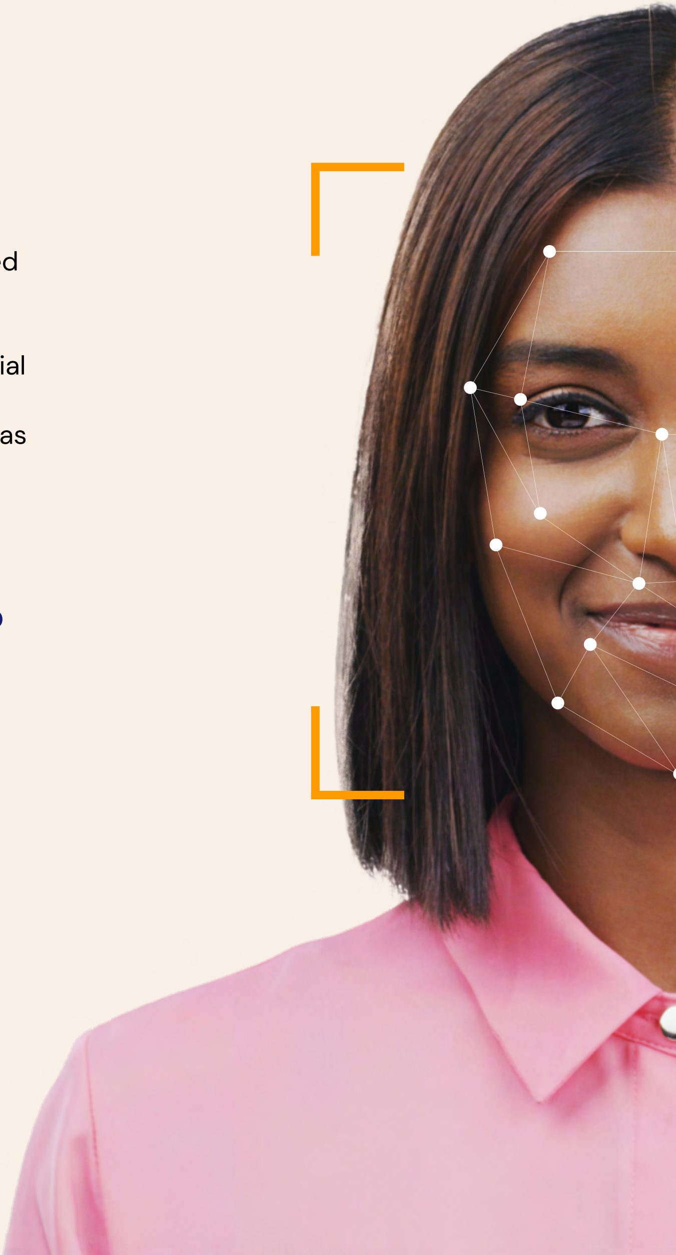
Fingerprint vs Facial Recognition

Two of the most prevalent biometric methods are fingerprint and facial recognition. Although fingerprint recognition has been around for a longer time, recent developments in facial recognition have given it the edge as the go-to option for scalable identity verification.

Fingerprint recognition has a reputation for accuracy, with studies putting results between 98% and 99.91%. However, it faces some challenges with scalability. Fingerprint scans rely on capacitive fingerprinting scanning, which essentially takes a picture of the finger, or ultrasonic fingerprint ID, which uses ultrasonic waves. Both technologies analyse details of the finger, including ridges, notches, and abnormalities, to find matches, and they rely on either high-resolution cameras or specialised hardware to capture the details of the finger properly.

Facial verification algorithms have improved greatly in the last few years. The recent proliferation of low-cost image-capturing devices (like mobile phones) providing facial image databases with many images, alongside GPU-based computing power, has allowed us to develop deep learning algorithms to perform facial recognition accurately and at scale.

When used to match subjects to clear reference images (like a passport photo or mugshot), facial recognition software can achieve accuracy scores as high as 99.97% on standard assessments like NIST's Facial Recognition Vendor Test (FRVT).



As a verification tool, faces are generally better than fingerprints because most smartphone cameras can capture more details of a face than a fingerprint;

this means that facial recognition technology can achieve higher accuracy rates, especially when people are verifying their identities remotely and don't have access to specialised fingerprint scanning hardware. Images used in facial recognition can also be obtained from cameras with varying levels of quality without a significant difference in accuracy.

Additionally, the popularity of the "selfie-style" picture format among smartphone users presents a non-intrusive, user-friendly way to capture facial biometric data. Most importantly, for companies that are scaling, facial biometric information can be verified from an ID document that carries an image of the holder. Biometric information can be collected from the user through a live-action (like taking a selfie) and compared to the biometric information on the document to see if there’s a match. For further security, facial recognition can also include liveness checks and anti-spoofing technology to ensure the user's authenticity.

	Fingerprint	Facial recognition
Unique identifier	✓	✓
Familiar to users	✓	✓
Requires ID access to verify	✗	✓
Accessible to all users	✗	✓
Can be done without specialised hardware	✗	✓
Does not require agents	✗	✓
Can work at a distance	✗	✓

Selfies vs Liveness

With facial recognition being the go-to option for biometric verification, businesses often have to make a choice between two kinds of facial verification methods: Selfies or liveness tests. Both options rely on the verification of facial features, taking into account factors like face detection, feature extraction, and an analysis of the distance between facial features.

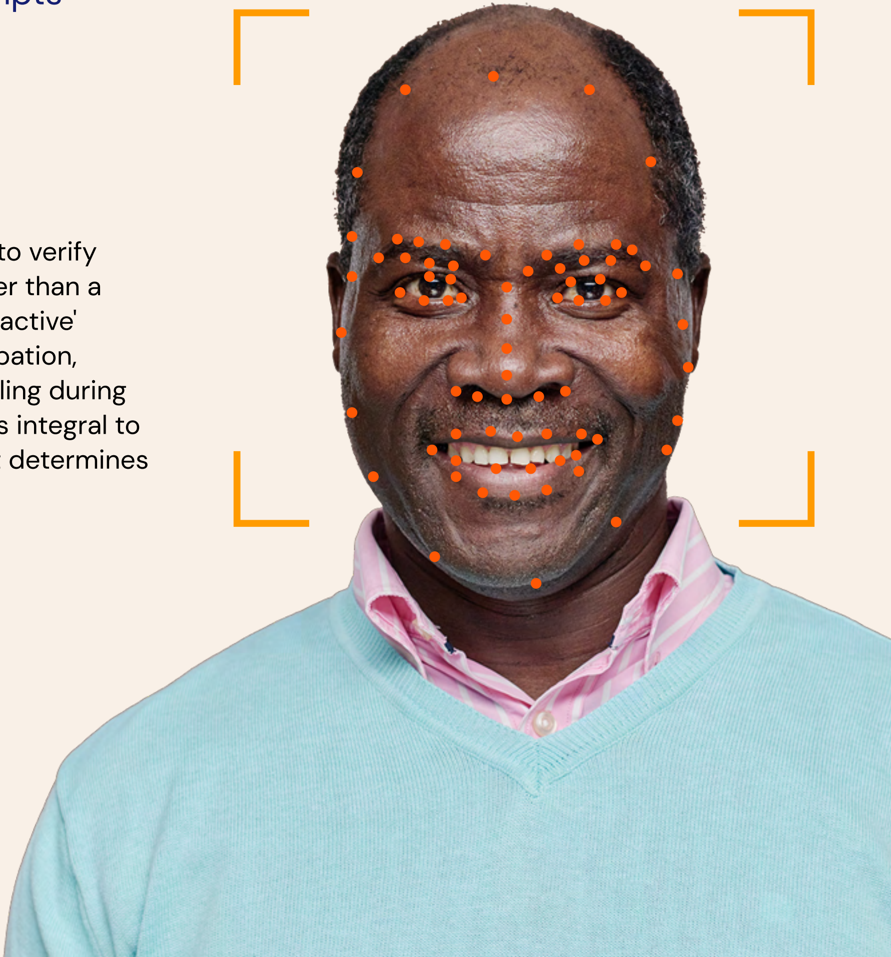
Selfie verification is straightforward – a user takes a selfie, which is then compared to a photo on an official document like a passport or driver's license. It relies on facial recognition technology to match facial features in both images. Selfie verification has the benefits of being a familiar, user-friendly process and being fast to authenticate. However, some selfie-verification algorithms can be vulnerable to high-level spoofing attacks, especially those using photographs or videos.

Liveness tests go a step further, requiring users to perform actions like blinking, smiling, or head movements. These actions enable the algorithm to determine if the selfie is being taken in real time.

These tests are harder to spoof because they require users to make real-time, spontaneous actions. Liveness tests provide better security with the ability to catch synthetic media and deepfakes.

87% of all biometric fraud attempts caught by Smile ID were only detected because of the active liveness component in our biometric solutions.

Active liveness is a technique employed to verify that a subject is a real, living person rather than a fraudulent or non-living entity. The term 'active' denotes the requirement for user participation, specifically involving actions such as smiling during the verification process. This technique is integral to a broader liveness detection system that determines the live status of an individual.



Smile ID × flutterwave

How Flutterwave built trust with users while reducing fictitious sign-ups by 90%

Goal

Fraud Prevention

Use case

Payments

Countries using Smile

South Africa Kenya Nigeria

The Problem

Flutterwave aimed to build trust in digital payments for new users, especially small business owners skeptical about online security and reliability, to increase confidence in their services.

The Solution

Flutterwave's implementation of Smile ID's **Biometric KYC** product which requires a user to take a selfie and compare that picture to the official government photo led to a **90% drop in fraudulent signups** and cut merchant onboarding from **24 hours to just 10-15 minutes**, boosting efficiency and speed. Smile ID can also run ultimate beneficial owner checks for the individuals behind these businesses. This deep level of due diligence helps Flutterwave build credibility and trust among its customers and protects them from nefarious actors.

Impact

- ☑ **90% Reduction** in fictitious sign-ups.
- ☑ **10 min** End-to-end merchant onboarding time.

Testimonial

"Smile ID has helped us verify different IDs in different markets. We find that the features they provide on their solution help make it easy to use just one provider to verify all of the IDs as opposed to using different providers, which is what we've done before now."

- Aramide Ayinla, Financial Crimes

Transaction Fraud

The ultimate aim for every fraudster looking to compromise an onboarding system is usually financial gain. This objective manifests through various sophisticated tactics that exploit weaknesses in the onboarding processes of financial institutions, e-commerce platforms, and other online services. The methods used range from identity theft and account takeover to more complex schemes like synthetic identity fraud.

1. Bonus/Referral Fraud

In Bonus/Referral Fraud, attackers exploit promotional offers designed to attract new customers or reward existing ones. This type of fraud typically involves creating multiple fake accounts to gain referral bonuses illegitimately. Fraudsters may use bots or automated scripts to rapidly create these accounts or recruit individuals to sign up using special referral links.

Bonus/Referral fraud becomes evident when many new accounts or referrals originate from similar sources, exhibit identical patterns of behaviour, or when payouts for referrals disproportionately increase.

At Smile ID, we have seen identity fraud spike up to 5 times the usual level during referral/bonus periods.

Deduplication has proven effective in helping to combat this kind of fraud. In practice, deduplication cross-references new signups against biometric data of previous signups and alerts businesses if the same data appears multiple times. Deduplication flags duplicate sign-ups regardless of country, ID type, ID number, name, or date of birth. It is the most effective deterrent for organised attacks on promotional signup codes.

At Smile ID, we have detected over 1.7 million duplicate faces for our customers using **Smile Secure**, our proprietary deduplication tool.

2. Account Takeover

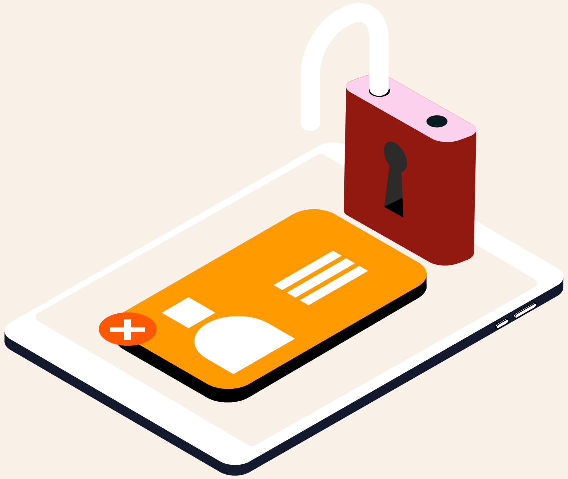
Account Takeover (ATO) happens when fraudsters gain unauthorised access to accounts by phishing, credential stuffing or exploiting vulnerabilities. The attacker gathers the victim's personal information, uses it to breach the account, and then makes unauthorised transactions, steals sensitive information, or uses the account for other illegitimate activities. Victims often realise they've been targeted when they notice unauthorised transactions, receive alerts for unusual activities, or find themselves locked out of their accounts.

Traditional means of authentication (passwords, PINs, and OTPs) that are still commonly used are not secure.

PINs and passwords are often weak and can be guessed or stolen from people. OTPs can be intercepted, and we have seen bad actors who work inside telecoms exploit their access to people's data to initiate and intercept OTPs and steal people's money and accounts.

To mitigate Account Takeover attacks, more businesses must implement risk-based analytics alongside multi-factored authentication that moves from traditional means of authentication to include biometric authentication that tests liveness and verifies a person's true identity in real-time. In addition, customer accounts should be monitored for unusual activities like logins from unknown locations or irregular transaction behaviour, which should trigger identity authentication measures to make sure that customer funds are safe.

Smile ID's Document Verification enables businesses to verify over 8,500 documents across 226 countries globally and the ability to add support for more documents upon request. It offers a robust way to confirm the authenticity of identity documents and establish ownership through selfie comparison—an ideal choice for standard onboarding and user authentication.



3. Money Laundering

Money Laundering in digital products often involves using online services to disguise the origins of illegally obtained money.

Fraudsters might funnel illicit funds through multiple accounts to hide their trail, including those in digital wallets, gambling, or cryptocurrencies.

This process typically involves a series of complex financial transactions designed to confuse authorities and make the money appear legitimate. Indicators of such activities include unusually large transactions, frequent transfers between accounts, or the use of shell companies and third-party intermediaries.

Businesses can mitigate money laundering attacks by conducting AML checks on onboarded customers to confirm if they are on any global watchlists and implementing risk-based security measures on high-risk customers.

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 on any of these lists, along with corresponding details. You can use information to evaluate the associated risks the customers pose.

4. Chargeback Fraud

Chargebacks occur when a consumer disputes a transaction from their issuing bank to obtain a refund because they did not initiate a transaction or, if they did, did not get value for the transaction. Consumers often initiate chargebacks because they never received the item or service or because it was not as described.

In many cases of chargeback fraud, the original owners of the account initiate the cashback dispute after their stolen details are used to carry out a transaction. In other cases, fraudulent customers can attempt to get a chargeback by insisting that they didn't get value for a transaction when they did.

Chargeback fraud affects companies across industries, including eCommerce, payments, wallets, card issuance, cryptocurrency, and more.

Like other kinds of fraud, chargeback fraud is much lower with verified customers. **Companies can mitigate it by implementing ongoing authentication on their users.**

Smile ID's biometric authentication solution enables businesses to safeguard accounts at login or during a high value transaction. It also creates time-stamped biometric proof that a transaction was authorised by the account owner in case of chargeback disputes.

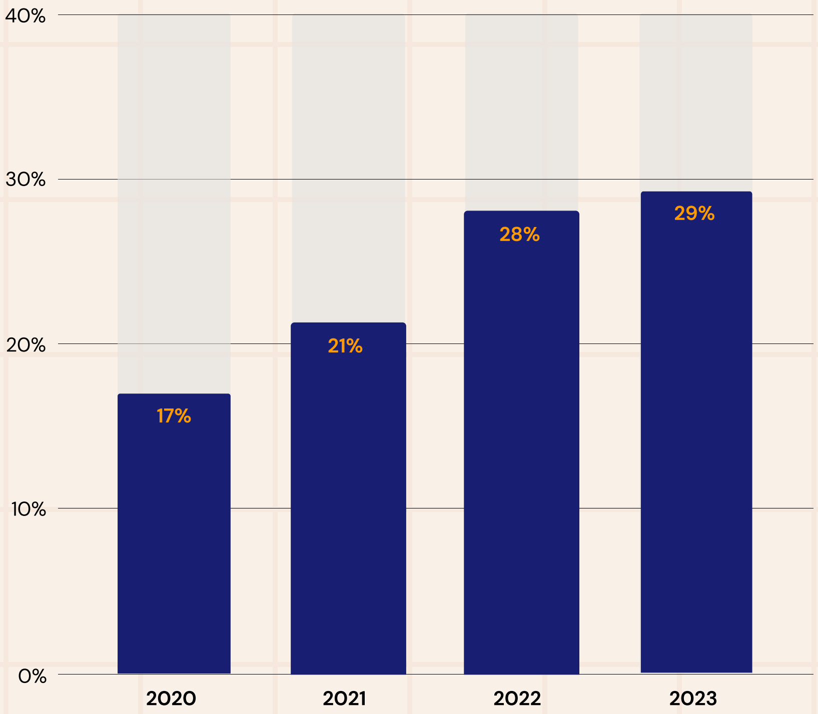
02

Impact of Fraud Across Africa

In 2023 we saw a 1% increase in fraud in absolute terms as a % of all KYC checks, with nearly a third of ID checks (29%) resulting in rejection. This statistic encompasses all failed ID verifications, including textual, document, and biometric checks.

Fraudulent attempts caught by Smile ID

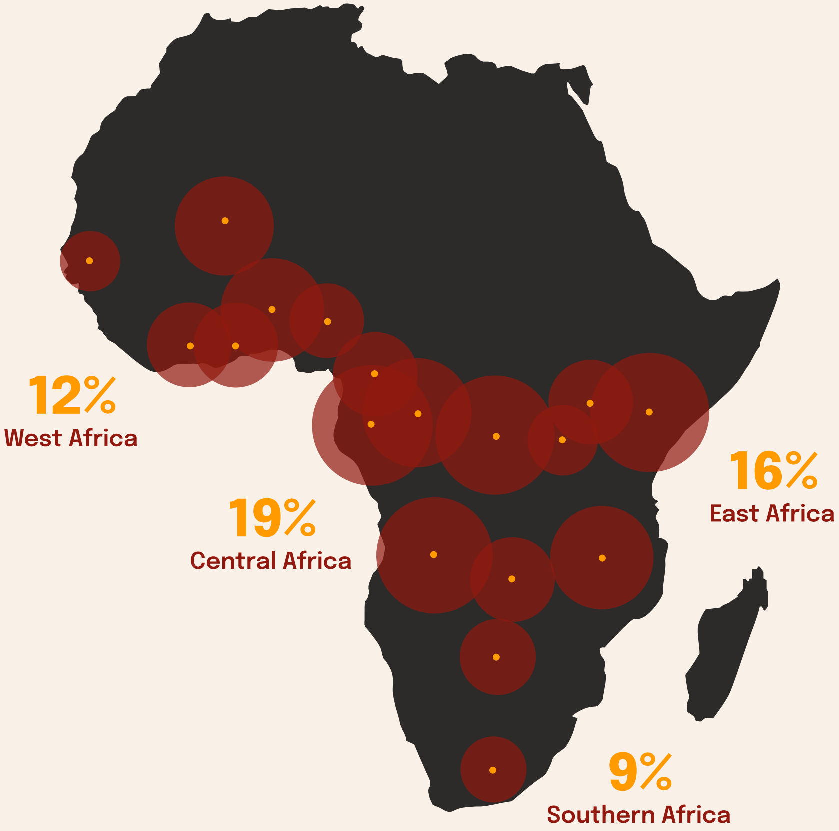
% of Total KYC Checks



Note on chart and data set:
This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from 2021 to 2023. Fraud analysis in this chart excludes the submission of invalid and poor-quality images.

Specific to biometric onboarding and document verifications, we saw the highest fraud rates in Central Africa at 19% between 2021 and 2023, followed by East Africa at 16%.

Notably, the nature of fraud is not static but dynamic; the past year witnessed a substantial rise in document and biometric fraud, with spoofing attempts particularly prevalent.



Note on chart and data set:
This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from 2021 to 2023. Fraud analysis in this chart excludes the submission of invalid and poor-quality images.

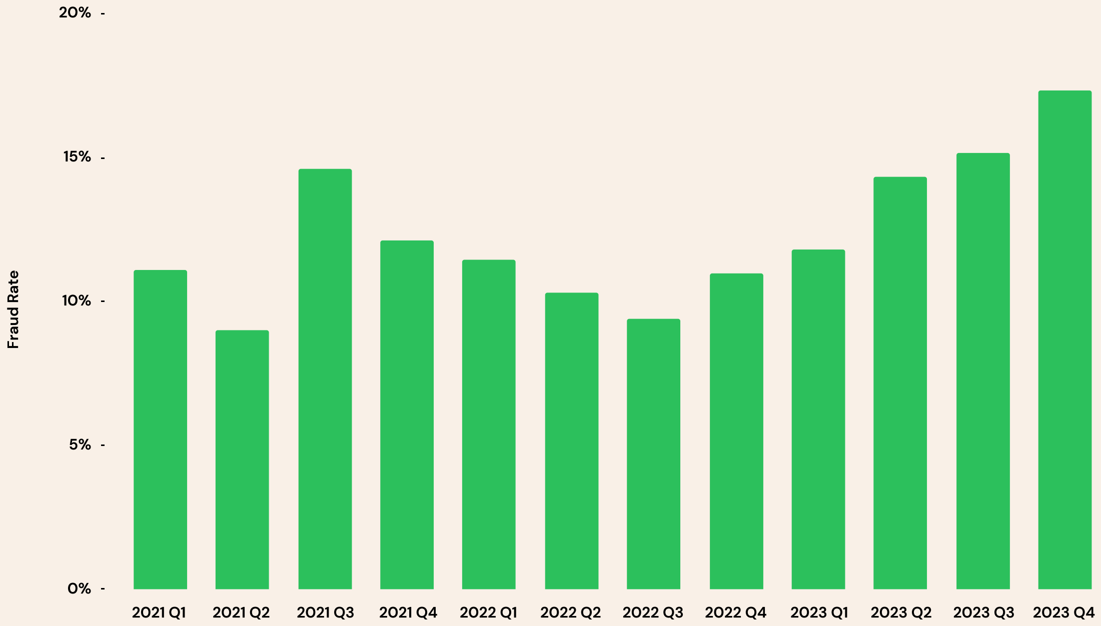
Biometric and Document Fraud in Focus

A quarterly analysis of biometric and document fraud data revealed that the overall rate of fraudulent document and biometric verification attempts has risen steadily over the last six (6) quarters, reaching an all-time peak of 17% in Q4 2023.

A monthly analysis of fraudulent activity in 2023 showed that fraud rates trended upwards over the course of the year before peaking in October.

While fraud rates increased over the general course of the year, they dipped between November and December, bucking a two-year trend of increased fraud towards the end of the year. We think this may be a result of fewer businesses running end-of-year promotional campaigns.

Average Biometric & Document Fraud Rate from 2021 to 2023



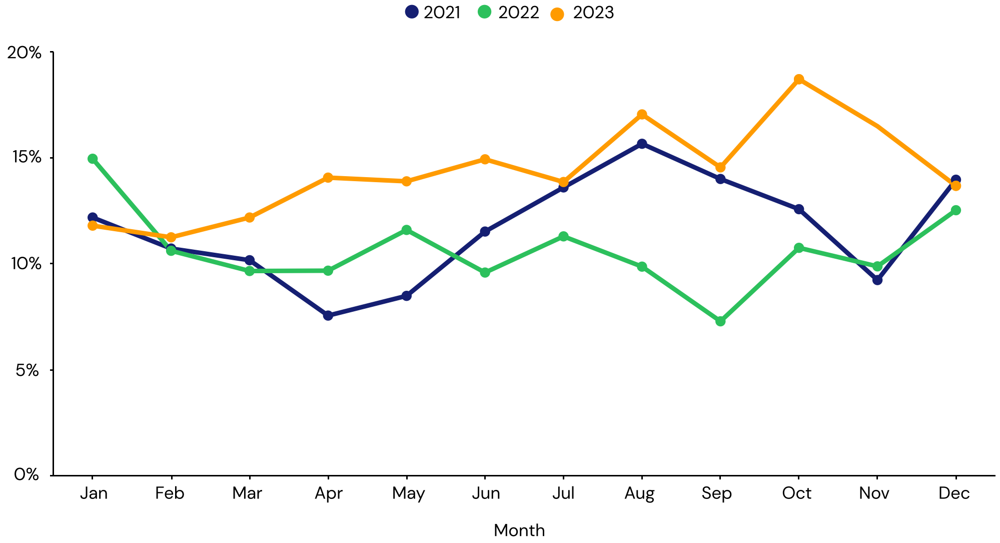
Note on chart and data set:
This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from Jan 2021 to Dec 2023. Fraudulent checks include biometric fraud, document fraud, and submission of invalid images.

A deep dive into the metrics around biometric and document verification brought up some interesting insights:

- **The rate of biometric fraud is consistently higher than document fraud indicating that identity theft is the favourite tool for identity fraud in Africa.**
- **In Q4 2023, attempted biometric fraud constituted a record-high 13% of all biometric verification attempts, contributing to the overall fraud spike in that quarter.**

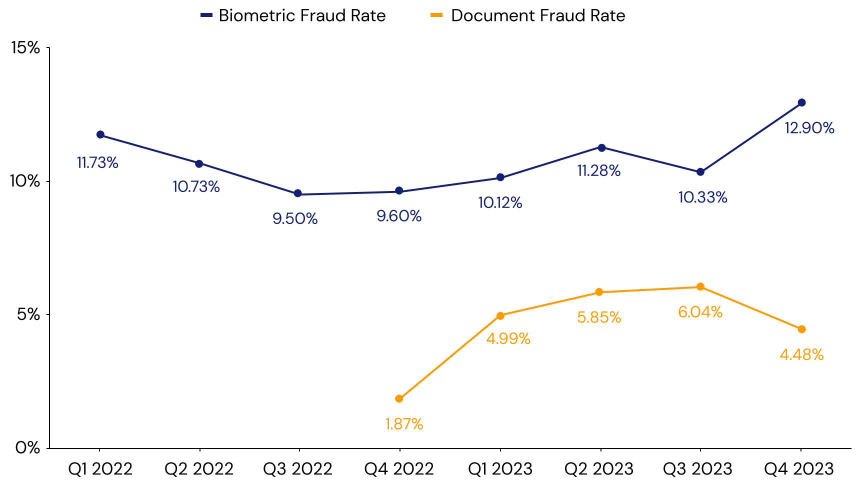
As our Document verification tool has a biometric component to it (selfie verification), these figures underscore the importance of layering biometric verification to any kind of textual or document verification.

Avg Biometric & Document Fraud Rate per Month for Smile ID Verifications



Note on chart and data set:
This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from Jan 2021 to Dec 2023. Biometric fraud includes fraud detected in Smile's biometric identification systems; document fraud refers to document manipulation or submission of unauthorized documents detected in Smile's document verification systems.

Fraud at a glance



Note on chart and data set:
This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from Jan 2022 to Dec 2023. Fraudulent checks include biometric fraud, document fraud, and submission of invalid images.

National ID card is Africa's most attacked document type

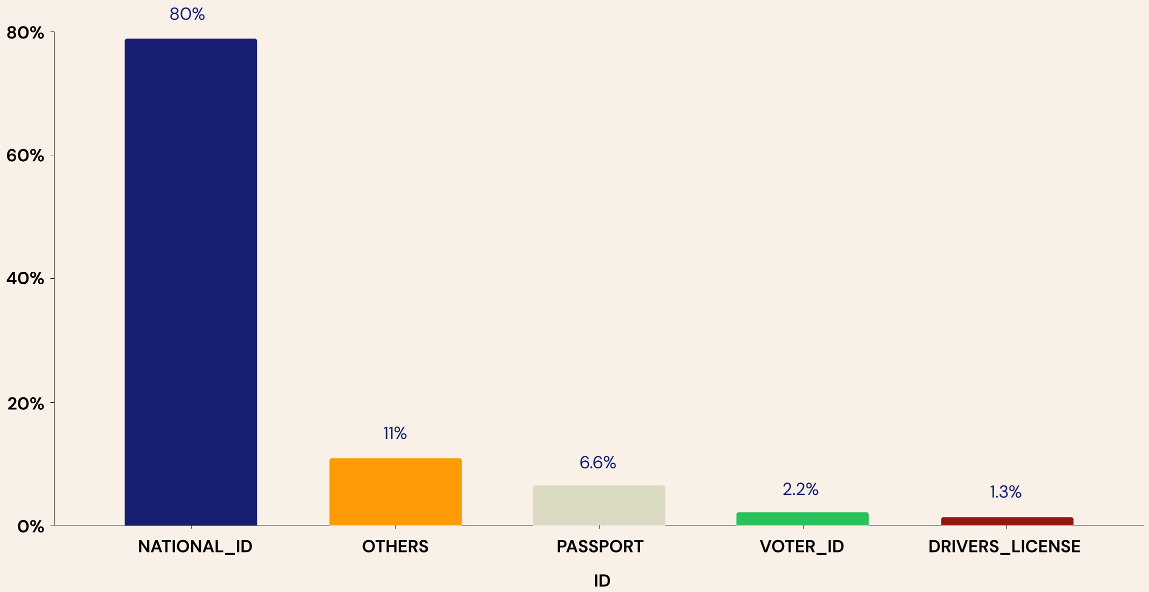
In the last two years, an overwhelming number of fraud attacks were directed at National ID cards, which accounted for 80% of all document fraud attacks.

11 out of the top 19 most attacked document types were also National IDs, with the Kenyan ID being the most vulnerable at a 25% fraud rate.

This preference for National ID cards among fraudsters results from two factors.

- In most countries, the national ID is the most common form of Government identification and is mandatory for most adults. With more national ID documents in circulation than ever before, the chances of them getting lost or stolen get increasingly higher by the year, exposing holders to potential document fraud.
- Many African countries have either recently implemented new national IDs or plan to in the coming years. Logistical issues around properly discarding the older IDs can lead to them falling into the wrong hands. An excellent example is South Africa, where the older Green ID card saw significant fraud targeting.

Fraud distribution by ID



Note on chart and data set:
This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from 2021 to 2023. Fraud analysis in this chart excludes the submission of invalid and poor-quality images.

19 Most Attacked ID Documents Across Africa

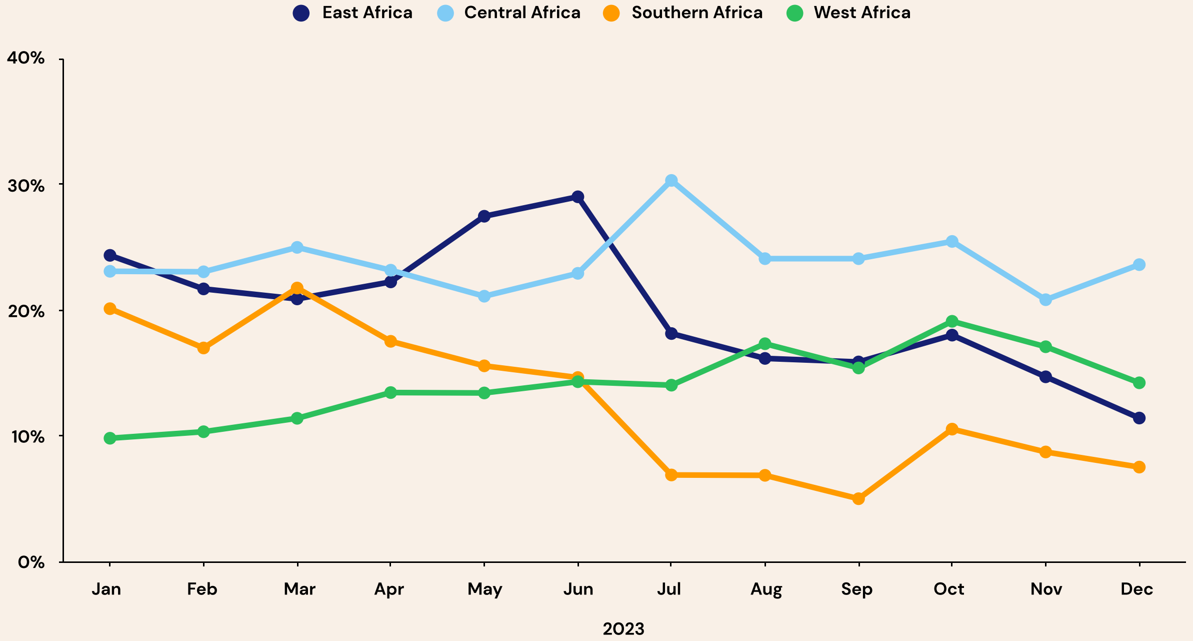
S/N	Document Name	Document type	Country	Attempted Fraud Rate
1	**Green Book**	National ID	South Africa	34%
2	**National ID card**	National ID	Tanzania, United Republic of	32%
3	**National ID card**	National ID	Kenya	26%
4	**National ID card**	National ID	Uganda	25%
5	**Passport**	Passport	Democratic Republic of Congo	23%
6	**SSNIT**	National Insurance	Ghana	20%
7	**Passport**	Passport	Malawi	19%
8	**Passport**	Passport	Ghana	19%
9	**National ID card**	National ID	Nigeria	18%
10	**Ghana Card**	National ID	Ghana	16%
11	**Drivers_license**	Drivers License	South Africa	14%
12	**National ID card**	National ID	Côte d'Ivoire	14%
13	**National ID card**	National ID	Cameroon	14%
14	**National ID card**	National ID	Cameroon	13%
15	**Voter ID card**	Voter ID	Nigeria	12%
16	**Passport**	Passport	Zambia	12%
17	**National ID card**	National ID	Benin	12%
18	**Passport**	Passport	Cameroon	11%
19	**National ID card**	National ID	Botswana	11%

Fraud in Africa through a regional lens

African countries have historically organised around geographical blocks. These geographic blocks share similar cultures and have in recent years created economic and political communities. Examining fraud trends across these regional blocks allows us to see what similarities, if any, lie along regional lines.

- Central and East Africa led the continent in average fraud rates over the course of 2023 with peaks of 29% and 30% respectively.
- Fraud rates in West Africa rose steadily over the course of the year and peaked at 17% in October before reversing for the rest of the year.
- Fraud rates declined in November and December for all regions under consideration except Central Africa.

Average Biometric & Document Fraud Rate per Month for Smile ID Verifications, by Region



Note on chart and data set:
This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from Jan 2021 to Dec 2023. Biometric fraud includes fraud detected in Smile's biometric identification systems; document fraud refers to document manipulation or submission of unauthorized documents detected in Smile's document verification systems.

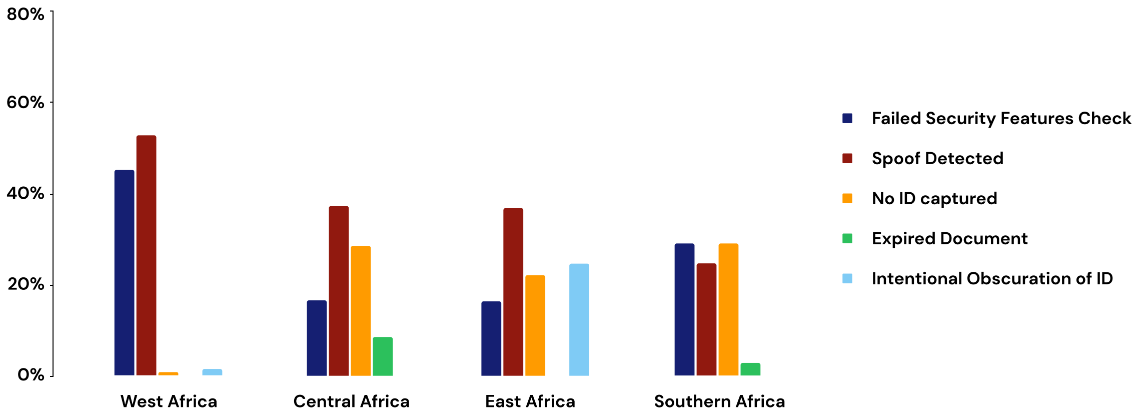
An overall analysis showed that in most cases of document fraud, no ID was captured meaning the user did not present an ID at all. This underscores the fact that document fraud in Africa is typically rudimentary, with fraudsters primarily depending on the absence of effective identity verification procedures within businesses.

In West Africa, however, most fraudulent documents were spotted because of failed security features, indicating a significant presence of counterfeit ID documents. The high occurrence of counterfeits suggests that fraudsters are exploring weaknesses in the ID document design.

Biometric fraud by region:

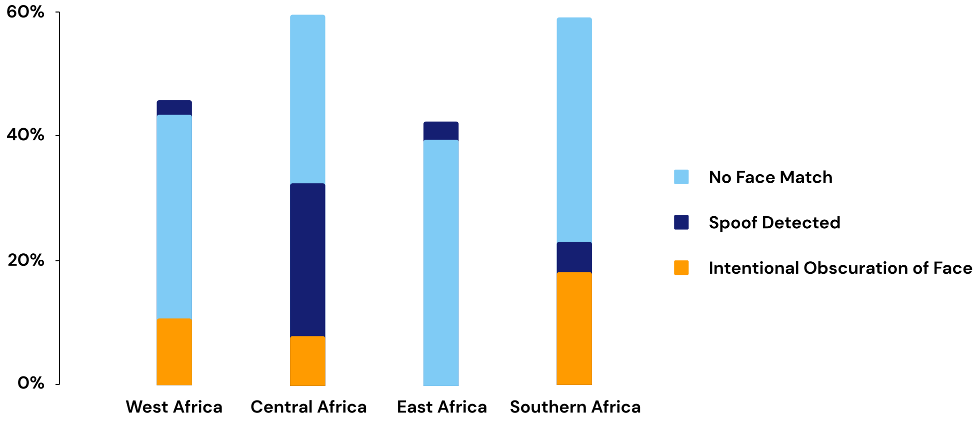
Across Africa, the most prominent indicator of biometric fraud was a no-face match, suggesting that the most common fraud was rudimentary; fraudsters didn't expend resources mimicking the true ID owners' faces. Spoofing attacks also featured prominently across the continent, edging slightly in West and East Africa.

Document Fraud by Region



Note on chart and data set:
This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from 2021 to 2023. Fraud analysis in this chart excludes the submission of invalid and poor-quality images.

Biometric Fraud by Region



Note on chart and data set:
This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from 2021 to 2023. Fraud analysis in this chart excludes the submission of invalid and poor-quality images.

Regional Insight: West Africa

Prominent Document ID Fraud: Failed Securities Check

Prominent Biometric Fraud Type: Spoofing

Countries in Focus: Nigeria Ghana

Identity fraud in West Africa is largely dominated by two countries, Nigeria and Ghana. Due to the broad adoption of digital and biometric ID verification in Nigeria, the use of physical documents is less common than in other markets.

However, Ghanaian ID documents have a higher fraud rate. The Ghanaian Social Security and National Insurance Trust (SSNIT), in particular, has the highest fraud attempt rate (20%). It is an old ID document being phased out in favour of the newer Ghana Card, which has advanced security features and a lower fraud rate.

Most attacked ID Documents in Ghana

ID Type	% of Volume*	Fraud Rate
SSNIT	2%	20%
Passport	3%	19%
Ghana Card	81%	16%

Most attacked ID Documents in Nigeria

ID Type	% of Volume*	Fraud Rate
National ID	0.1%	18%
Voter ID	3%	12%

* % of Volume of verifications

Regional Insight:
East Africa

Prominent Document ID Fraud: No Document Captured

Prominent Biometric Fraud Type: Spoofed Biometrics

Countries in Focus: Kenya Uganda

ID fraud in Eastern Africa reflects the overall trend across the continent, with national ID documents constituting the majority of document fraud attempts. Of the top 5 most attacked ID documents in the region, four are national IDs.

Overall fraud rates in Kenya remain stubbornly high. There are several contributing factors, one of which is the continued prevalence of old National ID cards which are constructed of black and white paper images, laminated in plastic. The newer Huduma Namba cards have faced several challenges to adoption, beginning with opposition in the courts to how the data was collected. The current government has announced more investment in, and consolidation of, existing ID systems in 2024.

Most attacked ID Documents in Kenya

ID Type	% of Volume*	Fraud Rate
National ID	96%	26%
Passport	1%	10%

Most attacked ID Documents in Uganda

ID Type	% of Volume*	Fraud Rate
National ID	21%	26%

* % of Volume of verifications

Regional Insight: Southern Africa

Prominent Document ID Fraud: Failed Securities Check

Prominent Biometric Fraud Type: No face match

Countries in Focus: South Africa Botswana

Owing to the size of its economy, fraud in South Africa has an outsized impact on the region representing almost 85% of the total fraud recorded by Smile ID. South Africa's developed digital ecosystem poses multiple opportunities for fraudsters to exploit. Botswana's National ID also witnessed a lot of attacks in the period under review.

Most attacked ID Documents in South Africa

ID Type	% of Volume*	Fraud Rate
Green Book	2%	34%
Driver's License	1%	14%
National ID	91%	7%

Most attacked ID Documents in Botswana

ID Type	% of Volume*	Fraud Rate
National ID	97%	10%

* % of Volume of verifications

Regional Insight: Central Africa

Prominent Document ID Fraud: No ID Captured

Prominent Biometric Fraud Type: No face match

Countries in Focus: Cameroon DRC Gabon

Central Africa bucks the trend of national IDs featuring predominantly among the fraudulent ID types as we saw other ID types like passports feature heavily in our analysis of most vulnerable documents.

A good example of this is the passport of the Democratic Republic of Congo, which has the highest fraud rates in the country and across the region. A similar trend is observed in Gabon, with international passports finishing the year as the document with the highest attempted fraud rate. In contrast, in Cameroon, the National ID is the most vulnerable document.

Most attacked ID Documents in Cameroon

ID Type	% of Volume*	Fraud Rate
National ID	86%	14%
Passport	10%	11%

Most attacked ID Documents in Democratic Republic of Congo

ID Type	% of Volume*	Fraud Rate
Passport	71%	23%

Most attacked ID Documents in Gabon

ID Type	% of Volume*	Fraud Rate
Passport	42%	15%

* % of Volume of verifications

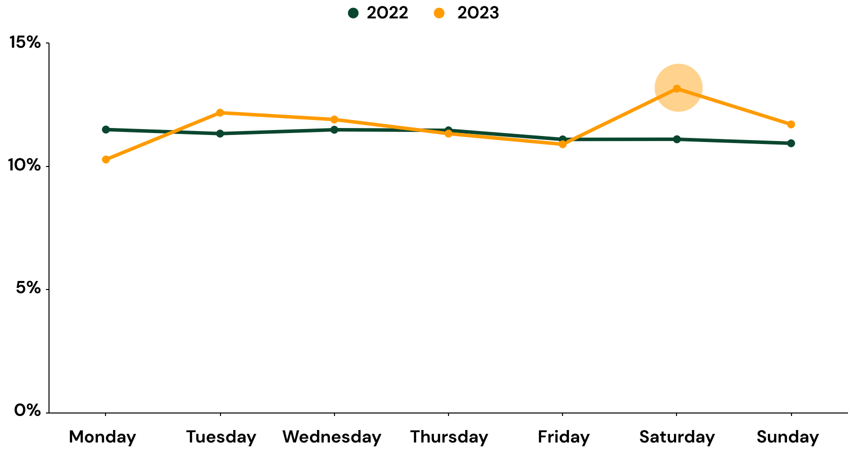
Time Analysis: How do fraudsters behave?

Our data analysis showed that fraud trends across days of the week differed significantly between 2022 and 2023.

In 2022, document fraud rates trended consistently throughout the week. However, in 2023, a shift in behavior was observed, with higher fraud rates being caught on Mondays and Wednesdays.

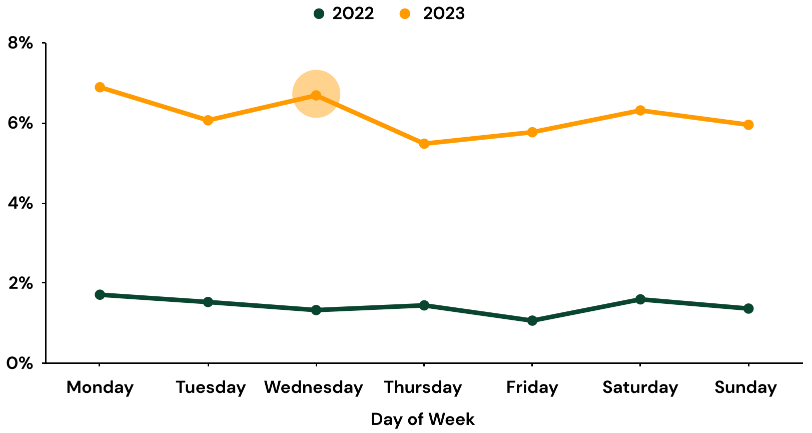
With biometric fraud, a similar trend is observed with consistent trend rates across weekdays in 2022 but significant variation in 2023. Fraudsters preferred weekends when committing biometric fraud in 2023.

Avg Biometric Fraud Rates for Smile ID Verifications by Day of Week



Note on chart and data set: This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from 2022 to 2023. Biometric fraud includes fraud detected in Smile's biometric identification systems; document fraud refers to document manipulation or submission of unauthorized documents detected in Smile's document verification systems.

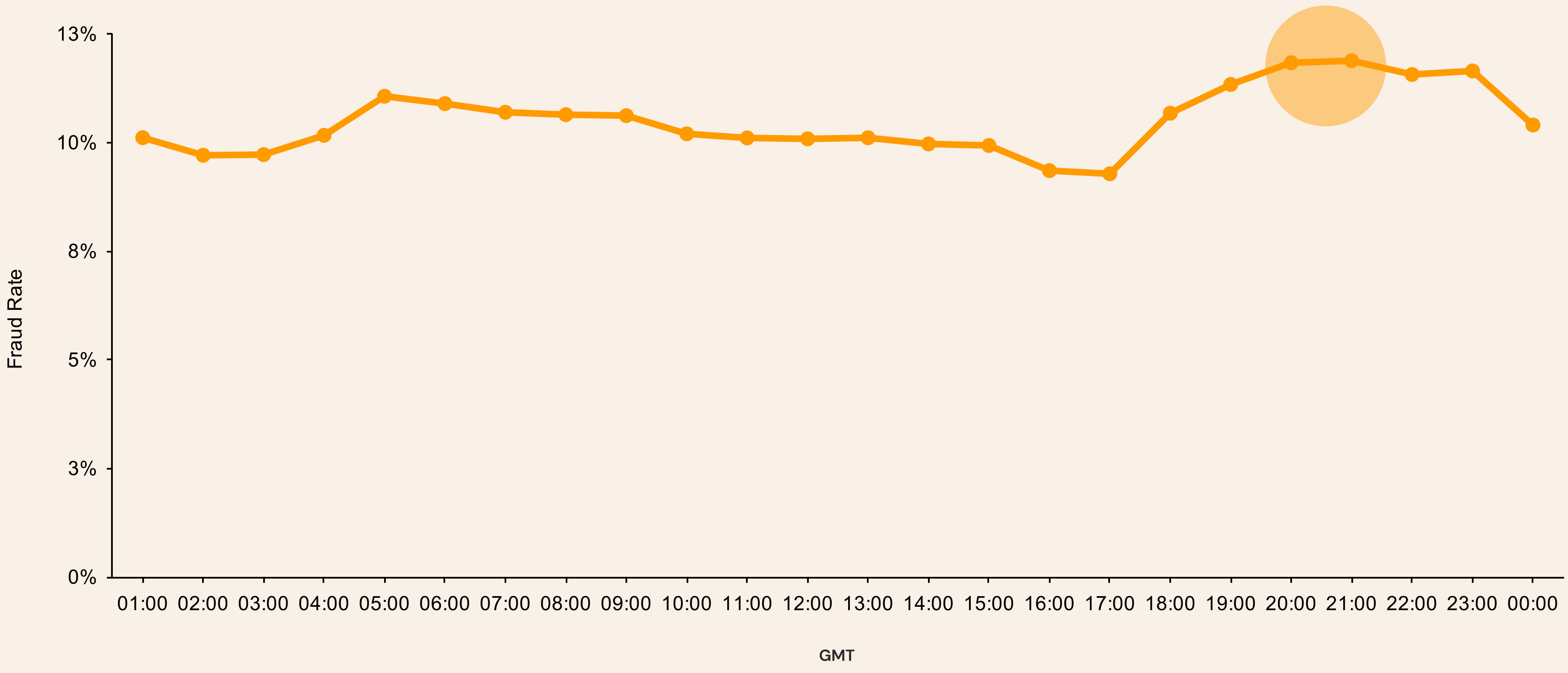
Avg Document Fraud Rates for Smile ID Verifications by Day of Week



Note on chart and data set: This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from 2022 to 2023. Biometric fraud includes fraud detected in Smile's biometric identification systems; document fraud refers to document manipulation or submission of unauthorised documents detected in Smile's document verification systems.

Fraud rises around 6pm GMT on most days, peaking at 9pm GMT, before starting to decline.

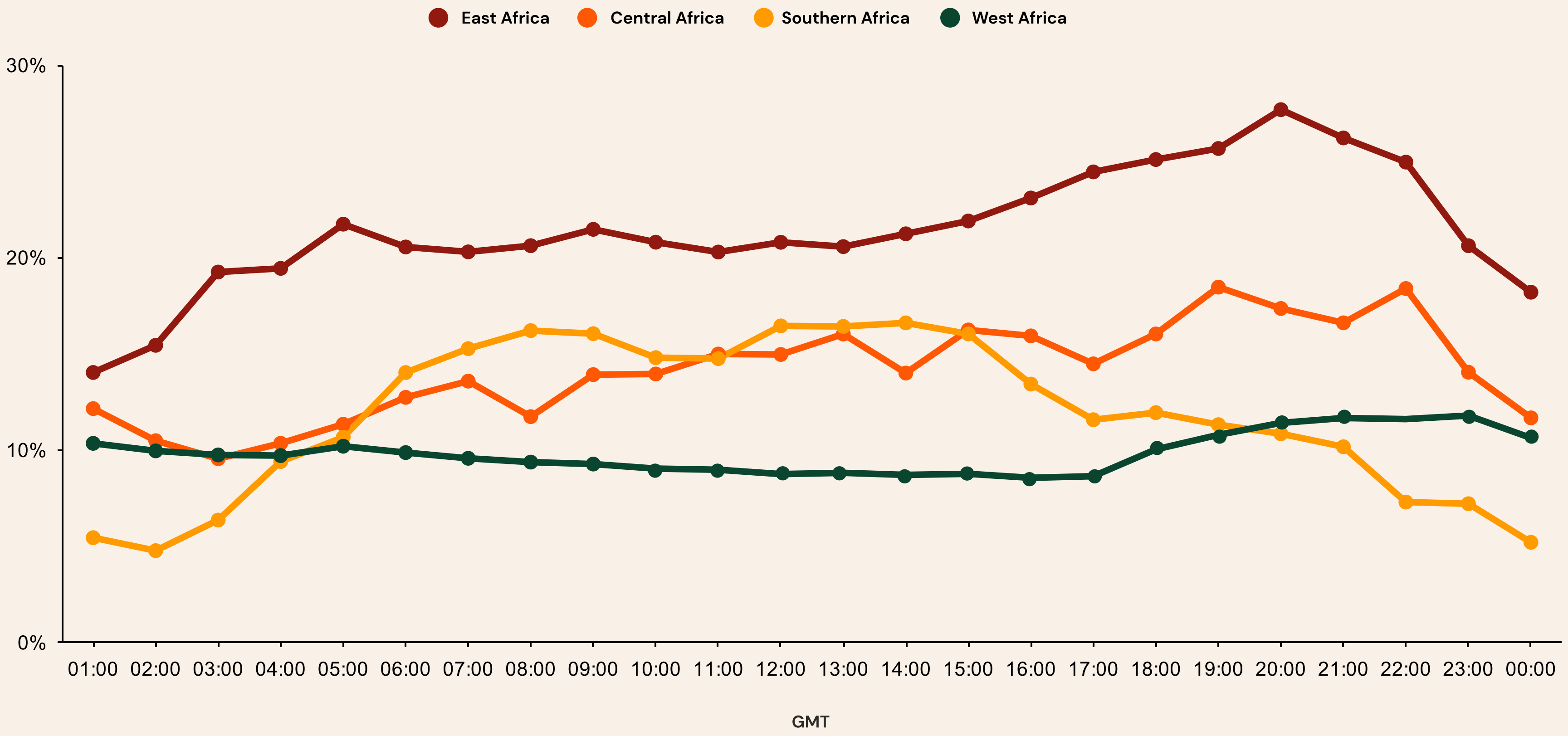
Fraud rate per hour



Note on chart and data set: This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from 2021 to 2023. Fraudulent checks include biometric fraud, document fraud, and submission of invalid images.

A regional analysis of the data reveals that fraud in all regions on the continent follow the same pattern except for Southern Africa where fraud appears to peak during midday between the hours of 8 am GMT to 2 pm GMT.

Fraud rate per hour, by region



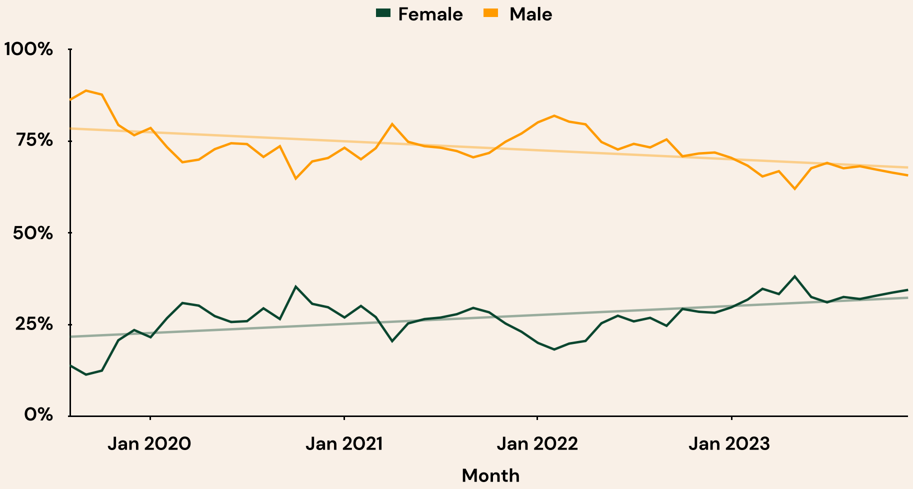
Note on chart and data set: This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from 2021 to 2023. Fraudulent checks include biometric fraud, document fraud, and submission of invalid images.

Gender Insights: Female IDs are targeted almost as much as Male IDs

Over the last few years, our verification data has shown a remarkable improvement in the inclusion of women, both financially and identity-wise. In 2023, we saw an overall rate of 35% of verified IDs belonging to women, a significant improvement from recent years and an indicator of progress towards equality.

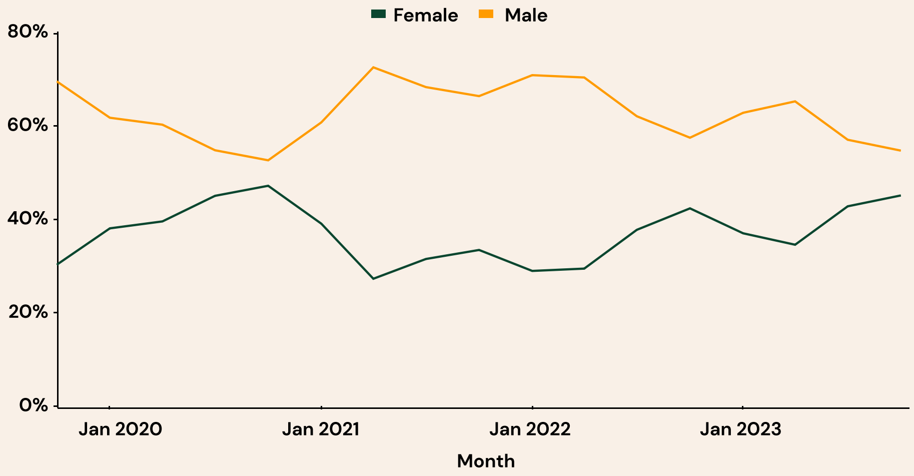
While we have historically seen more fraud attacks from male IDs, our 2023 data suggests that the gap in fraud attempts between genders is closing, with a difference in fraud rates by gender of less than 10% by year end. This is compared to the remaining 30% difference in volume of overall onboarding attempts by gender.

Gender distribution of Verifications Completed



Note on chart and data set: This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from all verifications completed by Smile ID from December 2019 to December 2023.

Gender distribution of Biometric Fraud



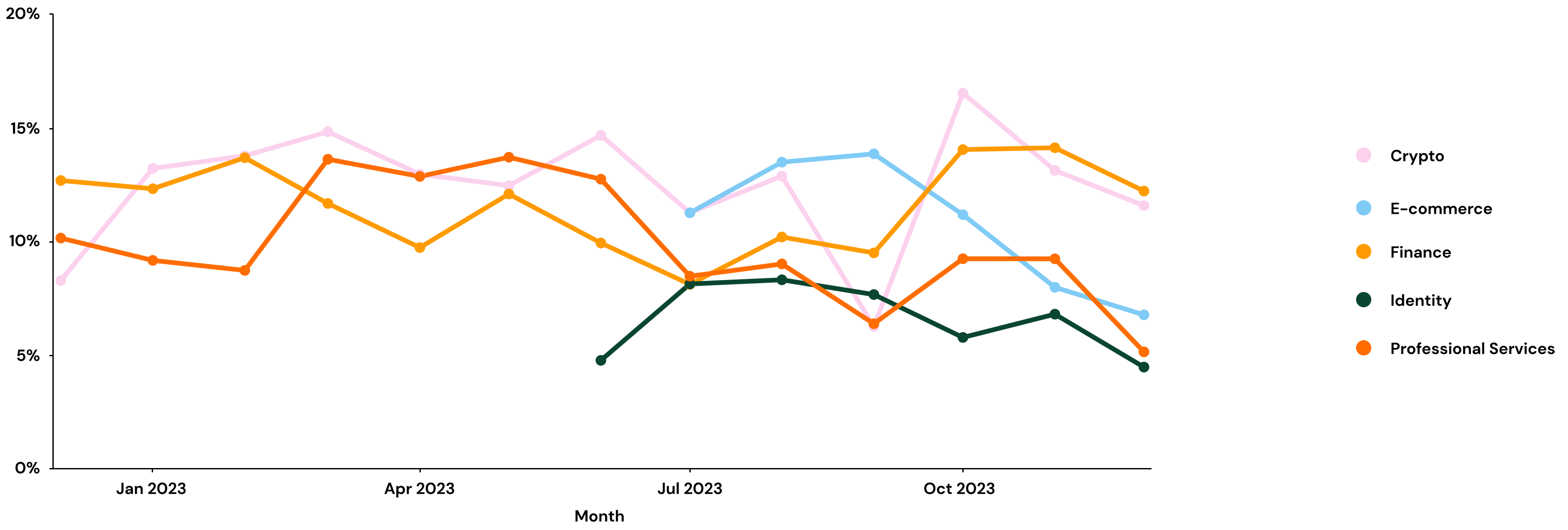
Note on chart and data set: This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from all verifications completed by Smile ID from December 2019 to December 2023.

Industry Insights

When we analysed data across industries, a few key insights stood out:

- In 2023, fraud rates across all industries varied significantly across the year in all industries.
- Companies in the crypto industry experienced the most fluctuation in fraud rates between 6% in September and around 16% in November.
- Fraud rates in the finance industry remained fairly constant between 10% and 15% over the course of the year.
- Fraud in all industries decreased in December, an indication that businesses may be running fewer promotions at the end of the year.

Avg Fraud Rate for Smile ID Verifications by Industry

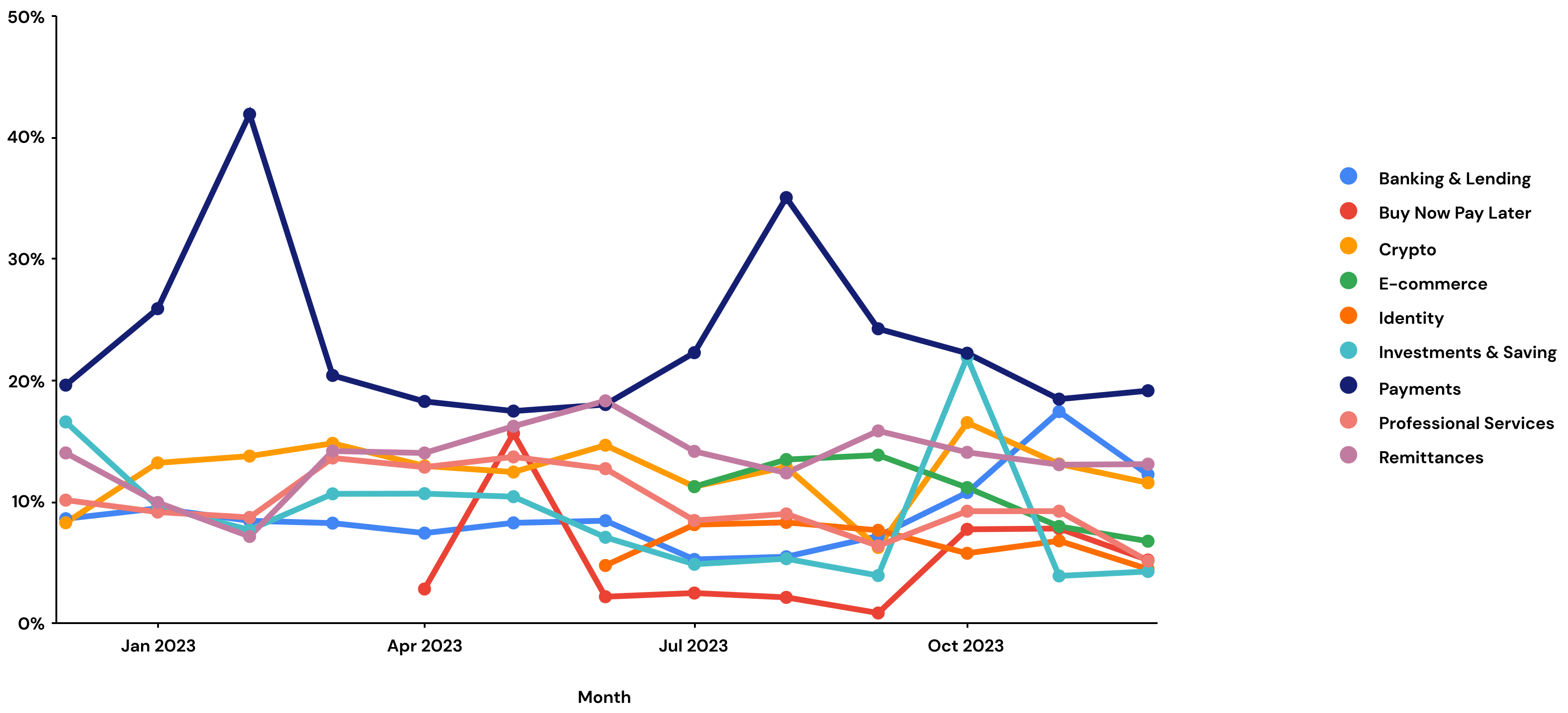


Note on chart and data set: This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from biometric and document verifications completed by Smile ID from Jan 2023 to Dec 2023. Biometric fraud includes fraud detected in Smile's biometric identification systems; document fraud refers to document manipulation or submission of unauthorized documents detected in Smile's document verification systems

While businesses in all industries can be victims of fraud, financial service businesses have long been the focus of fraudsters across the continent.

- The payments industry showed high levels of fraud, reaching as much as 42% in February 2023 and 35% in August.
- While the banking and lending industry saw consistent fraud trends over most of the year (under 10%), it experienced a spike at the beginning of Q4 2023, peaking in November at nearly 20%.

Avg Fraud Rate for Smile ID Verifications by Industry - Finance



03

Charting the Path

In 2024, businesses have a duty to customers and stakeholders to stay ahead of identity fraud. Fraud is constantly evolving, so businesses must be proactive in their approach to security. This section will address some steps businesses can take to stay ahead of the curve. Businesses can maintain trust and safeguard their reputation by prioritising security and staying informed about the latest fraud tactics.

Guide on how to set up a comprehensive anti-fraud system

While regulatory compliance is the bedrock of fraud prevention, it should only be treated as a minimum requirement. Businesses must go over and beyond regulatory requirements to protect the integrity of their products. Putting together a comprehensive anti-fraud system requires understanding the fraud risk points in any process. While it can differ significantly in practice depending on industry, the principles are largely the same.

High fraud risk points that businesses need to pay attention to are:

1. Onboarding:

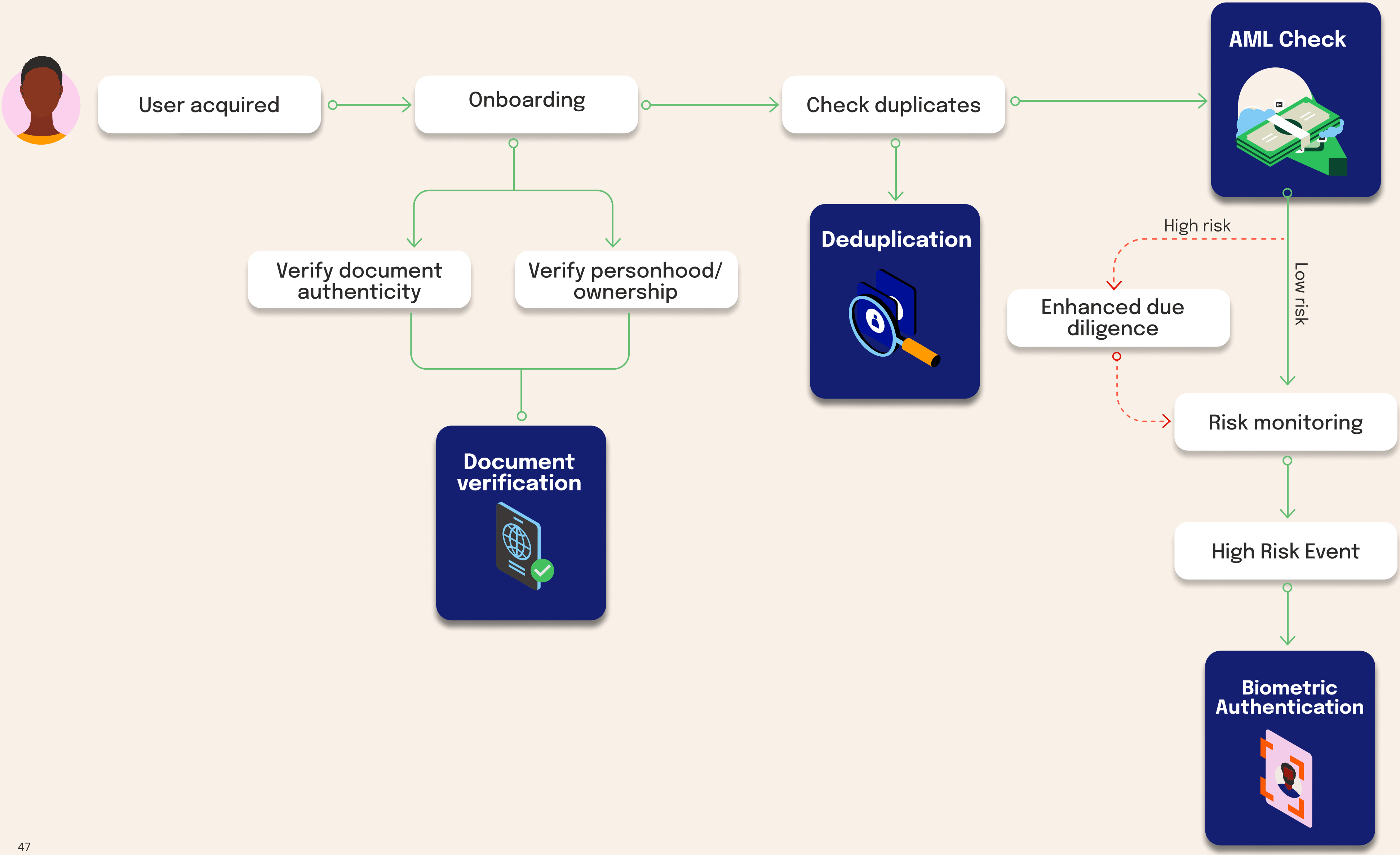
Stolen and fake identity attacks are most common in this stage, so we encourage businesses to implement a layered approach using the following measures:

- Use a document verification solution like Smile ID's that includes biometrics and allows you to both authenticate documents submitted and verify personhood/true ownership with a selfie or liveness test.
- Check for duplicate accounts using a biometric deduplication engine like Smile Secure.
- Use AML checks to verify that customers are not on any watchlists or sanctions lists.

2. High risk events:

These differ significantly depending on the industry. It could be high-volume transactions, increased velocity or frequent transactions or high-risk actions like password reset or new device initiation. During these events, businesses should perform ongoing biometric authentication on users.

How to set up a comprehensive anti-fraud system



Choosing the right KYC partner

Selecting the right identity verification partner is vital for businesses due to the legal and operational impact of KYC operations. A good partner facilitates scalable growth while ensuring regulatory compliance across jurisdictions. Conversely, choosing the wrong partner can lead to compliance issues, customer dissatisfaction, and legal consequences.

Ineffective KYC processes result in delayed onboarding, inaccurate verification, and heightened fraud risks. Evaluating potential partners based on track record, reputation, compliance capabilities, and solution flexibility is essential. Making an informed decision ensures a secure, compliant, and efficient customer onboarding process.

We created a step-by-step guide to help you figure out your unique business requirements and find a KYC provider that can best meet your needs.

Download it here.

Smile ID

Smile ID's 7-Step Guide

To Choosing a KYC Provider for a Pan-African Business

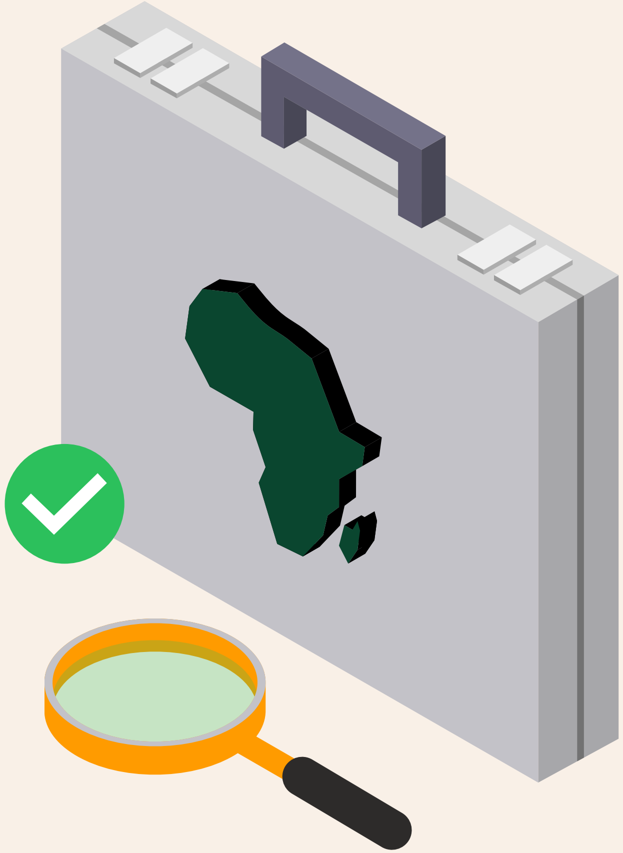
Need to outsource your business KYC needs? Here's a quick-read guide to help you choose the right partner for your business.

www.usesmileid.com

What to know when expanding across Africa

For businesses looking to expand across Africa, it is crucial to recognise the unique landscape of identity fraud within this region. Unlike other parts of the world, the trends and methodologies of identity fraud in Africa are distinct and complex, shaped by a combination of socioeconomic factors, regional variances, and technological disparities.

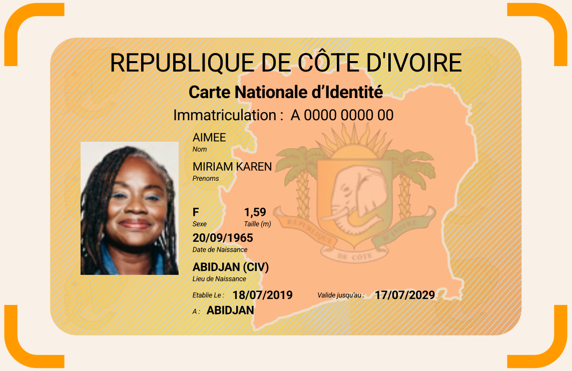
This section will explore how local customs, varying levels of digital infrastructure, and regional regulatory frameworks contribute to a unique fraud ecosystem. Understanding these nuances is a matter of safeguarding against risks and an opportunity to tailor approaches in fraud prevention and customer verification processes that resonate with the local context.



Biometrics is crucial to preventing Identity fraud

In the battle against fraud (identity or financial), biometrics is a non-negotiable tool, much more so in Africa, where the foundations of digital identity are still taking root. This evolving dynamic presents a unique opportunity for companies operating in the continent.

While navigating the diverse regulatory environment, businesses must leverage biometric technologies to enhance their fraud prevention strategies. Biometric systems, being more complex to falsify and closely tied to individual identities, offer a more secure and reliable verification method. Implementing biometric solutions not only aligns with the global trend towards enhanced digital security but also addresses the challenges faced in the African context, such as a high rate of identity fraud and a significant number of unbanked individuals. Businesses that adopt biometric verification systems are complying with emerging regulations and positioning themselves as trustworthy and forward-thinking entities.



REPUBLIQUE DE CÔTE D'IVOIRE

Carte Nationale d'Identité

Immatriculation : A 0000 0000 00

AIMEE
Nom

MIRIAM KAREN
Prenoms

F *Sexe* **1,59** *Taille (m)*

20/09/1965
Date de Naissance

ABIDJAN (CIV)
Lieu de Naissance

Etablie Le : **18/07/2019** *Valide jusqu'au :* **17/07/2029**

A : **ABIDJAN**

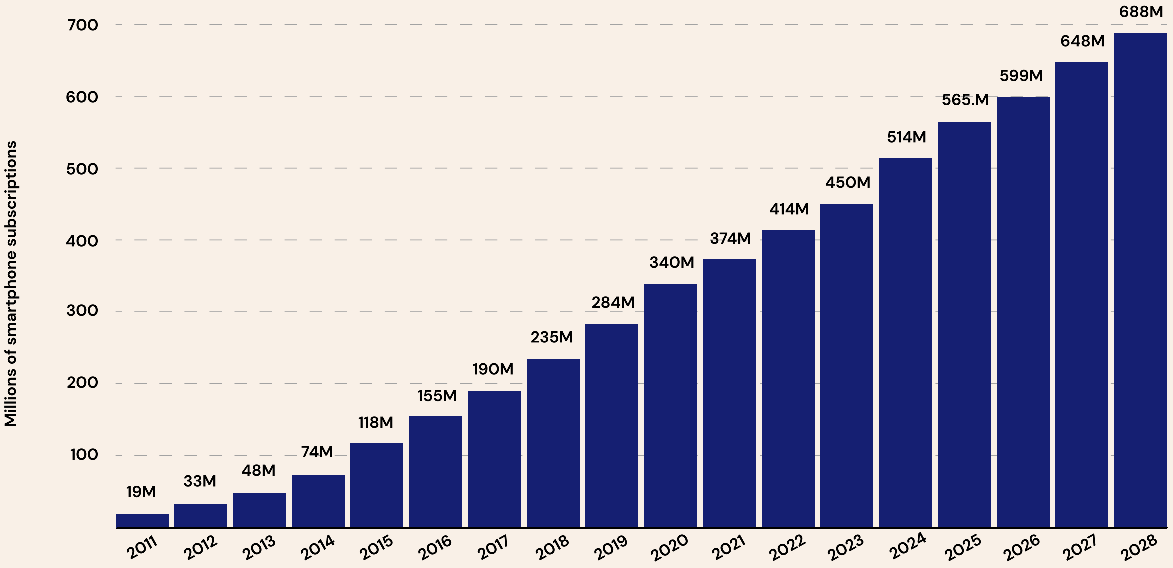
Mobile-first authentication is a priority

Africa is becoming an increasingly digital continent led by the proliferation of mobile phones. In 2023, there were an estimated 451 million smartphone subscriptions in Sub-Saharan Africa alone; that number is expected to reach 632 million in 2028. Many of Africa's digital subscribers use smartphones as a primary gateway to access the internet and essential services like banking, etc. With this in mind, businesses need to meet African users where they are with self-serve mobile-first authentication as a priority.

Although the agent-led approach may be useful, especially in rural regions with poor technology access, it can be fraught with challenges, including customers sharing personal information with agents who may sell it or use it for fraud.

A self-serve mobile-first authentication approach means that customers have the autonomy and security to verify their identity through their smartphones. This approach aligns with the growing preference among African consumers for digital solutions that offer convenience, speed, and security.

Smartphone Subscriptions in Sub-Saharan Africa by Year



Source: Statista 2024

SDKs are a better alternative to APIs for digital verification

When working with identity verification partners, businesses can choose to use either APIs or SDKs. While APIs provide considerable customisation potential, utilising them means your business may have to do a lot of heavy lifting to address the unique challenges of the African market.

On the other hand, SDKs can be engineered with these specific regional considerations in mind, offering a more tailored solution for verification purposes. For instance, SDKs can be equipped with a specialised capture screen designed to illuminate the user's face, ensuring the capture of high-quality selfies, even in areas with poor lighting. They can also be engineered to capture images that are both high in quality and suitably sized for transmission in areas with limited connectivity.

Unlike APIs, which require constant communication with a server, SDKs can be built to handle intermittent connectivity through offline functionality or data caching. They can be customised to handle retries and errors, which are crucial in environments with unstable network conditions, ensuring a smoother, more reliable user verification process.

At Smile ID, we tailor our SDKs for the African Market

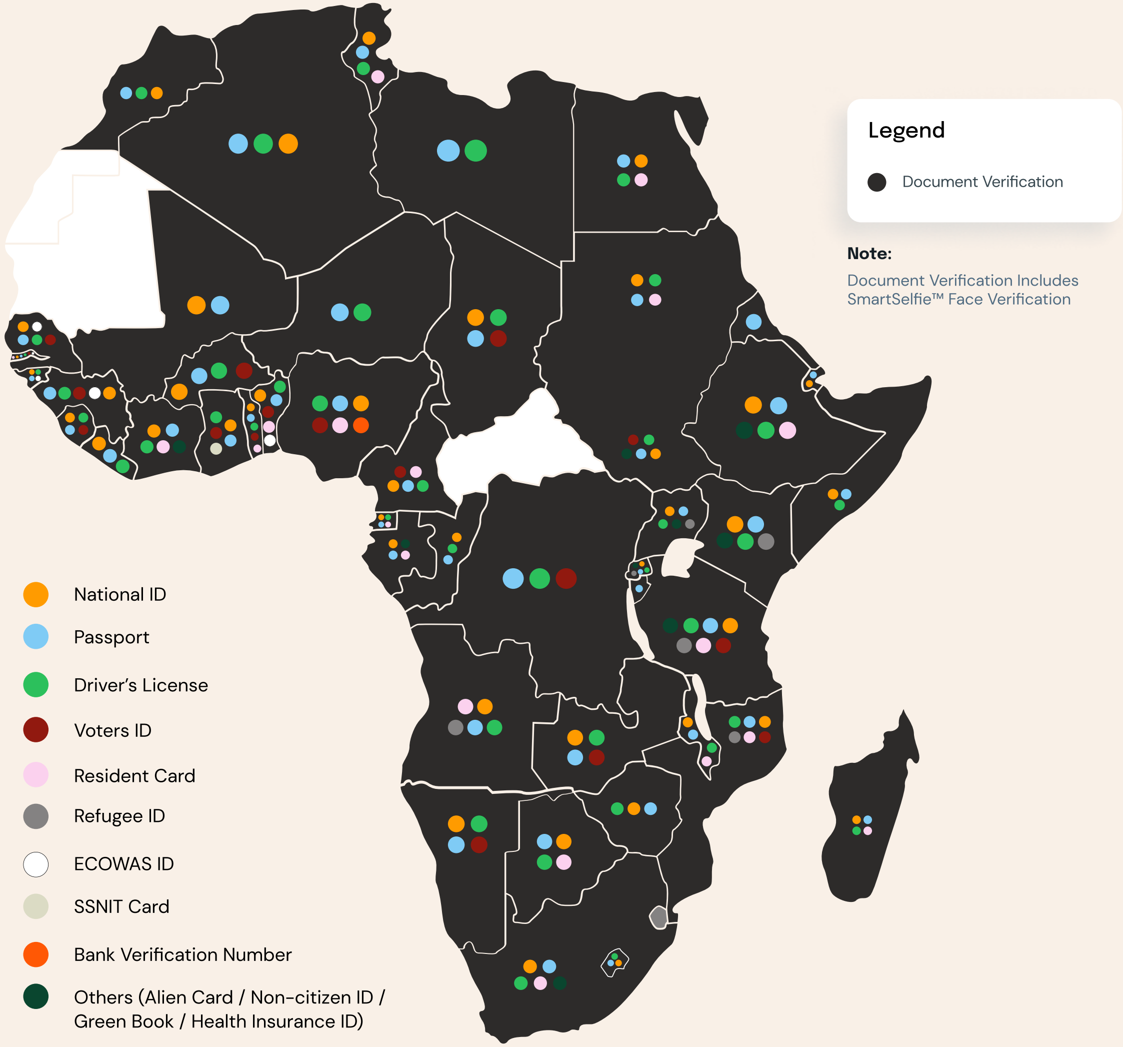
To optimise our SDKs for the unique requirements of the African market, we’ve incorporated several key considerations, some of which include

Device Considerations:	Many African customers have phones with restricted storage capacity, so we’ve designed our mobile SDKs to be as compact as possible to minimise the impact on the app sizes of our partners. In addition, our SDKs maintain compatibility with a broad range of devices, supporting Android 5 (released in 2014) and iOS 12 (2018), and we optimised our image captures by employing compression techniques that produce smaller file sizes without imposing minimum resolution requirements.
Challenging Lighting Conditions:	Poor lighting, particularly at night, often results in low-quality selfies, so our SDKs’ selfie capture screens are designed to illuminate the user’s face with their background, enhancing the likelihood of obtaining a clear photo.
Agent-Led Scenarios:	Many businesses in Africa employ agents to provide services to their clients. Our mobile SDKs accommodate this by enabling agents to use the rear camera to capture user photos without handing over the device.
Connectivity Optimizations:	Our solutions are optimised for low bandwidth environments, high latency, and flaky connections. By enabling multiple retries in case of network failures and reducing image size, we optimise our services for challenging conditions. Furthermore, our SDK continues to operate even without an internet connection. Therefore, the user can still capture images without the internet and they will be submitted once the device is back online.

Varying KYC/AML Regimes Will Be a Challenge

Africa's diverse regulatory landscape remains a significant challenge for companies expanding across the continent. Each African country has its own set of regulations and compliance requirements, and companies must invest in comprehensive research to understand the specific KYC/AML frameworks in each target market.

When outsourcing ID verification, businesses should look for partners with extensive coverage and local expertise around the continent. An ideal ID verification partner should provide solutions with sufficient geographical coverage and advice on the local regulatory landscape in countries your business is expanding to. This prevents the need for multiple integrations, allowing companies to expand to new territories with minimal technical work.



Note:

Document Verification Includes SmartSelfie™ Face Verification

04

Future Outlook

This section explores the impact of technological advancements like AI and machine learning and the increasing role of digital identity verification methods. It also discusses anticipated regulatory shifts and their implications for businesses and consumers, setting the stage for a comprehensive understanding of the future fraud prevention landscape.

Radical Expansion in Synthetic Identity Attacks

The rapid advance and accessibility of AI tools is reducing the cost of sophisticated fraud. In 2024 we expect to see substantially more synthetic identity fraud in Africa. These attacks often combine hyper-realistic deepfakes with stolen ID credentials obtained via the web or data leaks.

Although there hasn't been a significant uptick in synthetic identity fraud on the continent, global fraud trends already indicate that fraudsters are increasingly using deepfakes to try and beat biometric checks including liveness checks. As AI solutions become more accessible and the skill requirements lessen, more of these kinds of attacks are expected.

These attacks may include the use of multi-modal deepfakes, combining audio and video to create highly realistic content that cannot be easily identified by humans alone. More sophisticated identity theft attempts and financial scams that test the limits of today's identity verification protocols will evolve. Social engineering and phishing attacks are also expected to become more difficult to spot as people will struggle to tell the difference between deepfakes and real media. The realistic nature of these deepfakes may also cause an erosion of trust in digital services.

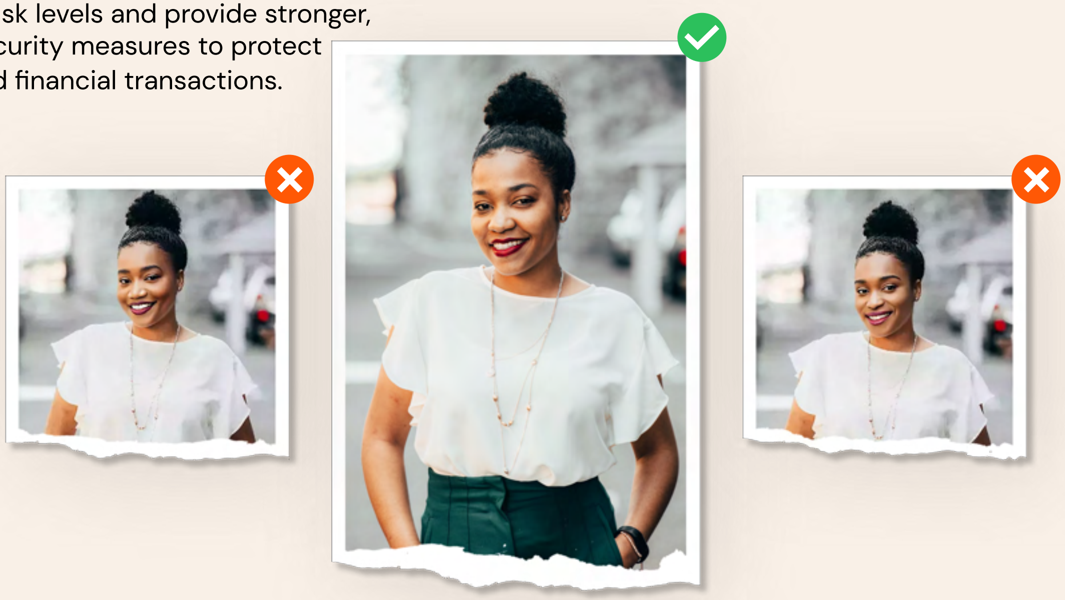
AI will be integral in the fight against fraud

As fraudsters become more sophisticated, so will the AI-driven technologies designed to thwart them. AI will enable the constant monitoring of user activities and transactions, providing real-time alerts for suspicious behaviors and potential fraud. This level of vigilance is crucial in the fast-paced digital world where threats can emerge rapidly. By analyzing patterns in user behavior, AI systems can identify deviations that may indicate fraudulent activities, offering an additional layer of security.

Active liveness detection systems, where users are required to perform specific tasks, will be more widely implemented. These tasks ensure that a real, live person is present during verification, significantly reducing the risk of spoofing and impersonation by deepfakes. Advanced anti-spoofing models will be developed to combat new and evolving methods of identity fraud. AI will be pivotal in detecting deepfakes with accuracy far surpassing human capabilities. This includes identifying even the most subtle inconsistencies and anomalies in synthetic media. Generative Adversarial Networks (GANs).

AI will also help establish trust in digital interactions by analyzing data provenance – the history of data including its origins and changes over time. This includes tracking specific devices used, locations, and consistent behavior patterns of users. By assessing historical data, AI systems can create reliable trust profiles, making it easier to identify legitimate users and flag potential fraudsters.

We can also expect AI integration with other state-of-the-art technologies, such as blockchain, to provide secure and transparent digital transactions. Multi-factor and adaptive authentication systems, bolstered by AI, will become more prevalent. These systems will adapt to various risk levels and provide stronger, more nuanced security measures to protect user identities and financial transactions.



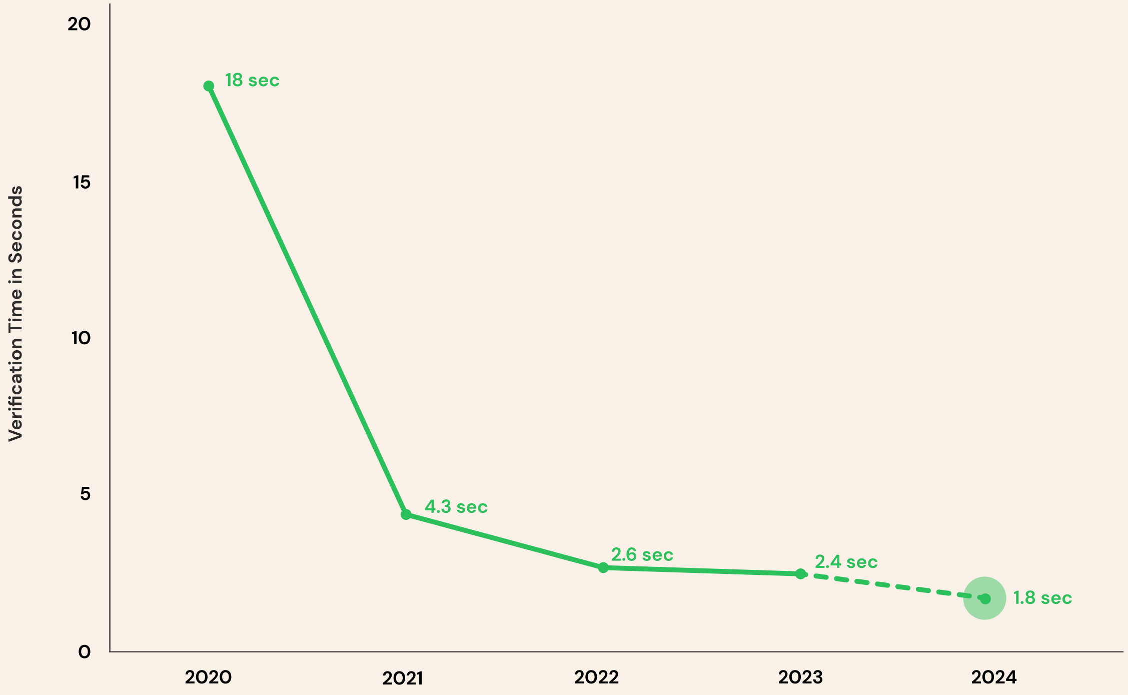
Significant Acceleration in Performance

Looking ahead we expect to see a continued decline in median verification time.

In response to growing demand and feedback from verification providers like Smile ID, African ID authorities are investing in server capacity and designing systems based on performance rather than politics, resulting in better uptime and API responsiveness.

On the commercial side, Smile ID is seeing more global companies enter Africa and demand the same levels of performance as in the US, Europe or Asia. In response Smile ID has invested in new mobile SDKs, purpose-built APIs for volume and server-side optimisations to handle exponential scale. As a result, we expect to see median verification times cross the 2 second mark by the end of 2024, with some products like authentication, clocking sub-second responses.

Smile ID's Median Verification Time by Year



Note on chart and data set: This report uses anonymised data collected from transactions on Smile ID. Data in this chart was collected from all verifications completed by Smile ID from 2020 to Dec 2023.

When it comes to user safety, trust the experts

Trusted partner

On-the-ground team in 11 countries

Award winning provider

Voted #1 for 'Excellence in KYC 2023'

Unbiased models

Facial verification models are trained on African faces

Local experts

Close regulatory and government relationships

Africa focused

Products and features built for Africans

You'll be in good company

Some of the fastest growing businesses across Africa trust Smile ID to fuel their growth.

paystack shara Uber BINANCE Stanbic IBTC A member of Standard Bank Group Moniepoint verto

OPay Bolt FairMoney LUNO LipaLater PATRICIA iKhokha

paga angaza kuda. flutterwave Yellow Card Kudi branch

RAENEST Sterling PenCom NATIONAL PENSION COMMISSION umba miterahealth® Cellulant onafriq Previously MFS Africa

WOWZI d.light FCMB GTBank ImaliPay koa Bridgecard ZENITH

Financial Services ✓ Health ✓ Transportation ✓ Buy Now Pay Later ✓ Energy ✓ Education ✓ E-Commerce ✓

We enable our partners to onboard good users fast & detect fraud at scale.

MarketForce

Onboarded merchants in **10 milliseconds**

Bridgecard

Reduced card creation downtime **by 41%.**

flutterwave

Reduced fictitious signups **by 90%.**

paga

Reduced onboarding time from **2 hours to 7 mins.**

Yellow Card

Automated KYC in **16 countries** while staying compliant.

ImaliPay

Onboarded users in **less than 10 seconds.**

umba

Reduced fraud by 90% using biometrics.

kuda.

Full digital bank accounts in **under 30 minutes.**

FairMoney

20x daily loan disbursement number since integration.

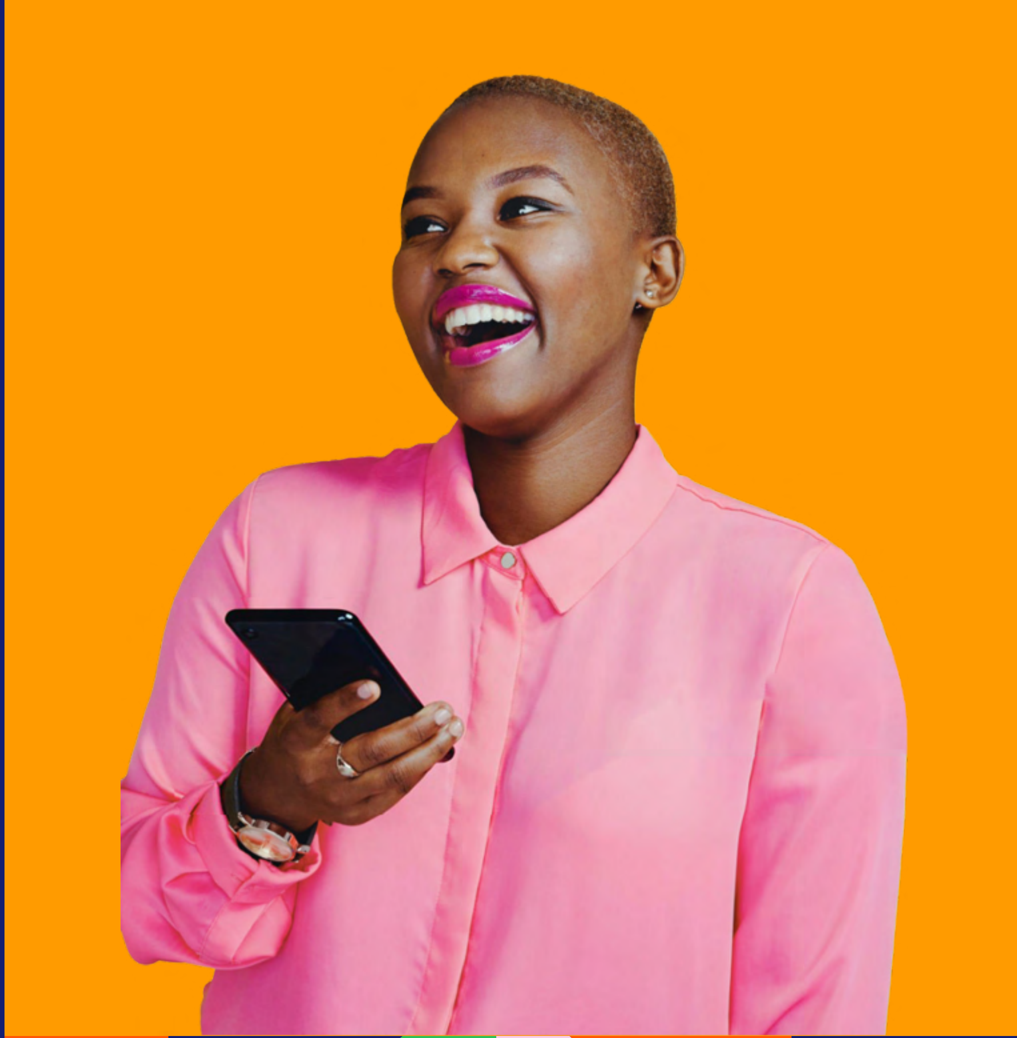
www.usesmileid.com

Contact Us

Talk to a Smile ID expert & discover how our all-in-one KYC/AML solution can help you verify users and merchants across Africa with ease.

Book a Call

Smile ID



Contributors

Kai Tyng Loh

Head of Analytics

Lameck Orina

Graphic Designer and Illustrator

Mark Straub

Chief Executive Officer

Peace Itimi

Director of Marketing

Orahachi Onubedo

Content Marketer

Appendix I - Glossary of Common Terms and Their Definitions

- **Active Liveness:** verification process where the user must perform actions to prove their presence.
- **AML/CFT:** Anti-Money Laundering/Combating the Financing of Terrorism; regulations to prevent illegal money transactions.
- **API:** Application Programming Interface; a set of protocols for building software and applications.
- **Authentication:** the process of confirming user identity.
- **Biometric Authentication:** Verification process using biometric data like fingerprints or facial recognition.
- **Biometric Fraud:** Illegal activities involving the misuse or impersonation of unique biological traits, such as fingerprints or facial recognition data.
- **Churn:** Rate at which customers stop using a service.
- **Deduplication:** the process of removing duplicate data.
- **Document Verification:** Confirming the authenticity of identification documents.
- **Duplication:** The presence of identical data or entries.
- **Fraud:** Intentional deception for gain, increasingly sophisticated in digital environments.
- **Friction:** User experience challenges, particularly in authentication processes.
- **GMT:** Greenwich Mean Time, a time zone reference.
- **GPU:** Graphics Processing Unit used in computing for rendering images.
- **High-risk event:** A situation with a high potential for fraud.
- **ID document:** An official document proving an individual's identity. It is typically government-issued.
- **Identity Fraud:** The illegal use of someone else's identity.
- **KYC:** Know Your Customer, a process for identity verification.
- **Liveness:** Technology to ensure the subject in a biometric scan is real and present.
- **NIST:** National Institute of Standards and Technology. An American organization setting technology standards, influential in biometric verification.
- **Optical Character Reading:** The process of converting images of text to machine-encoded text, used in document verification.
- **Onboarding:** The process of integrating new users, critical in user experience and security.
- **Risk Monitoring:** The continuous analysis of operations for potential security threats.
- **SDK:** Software Development Kit, a set of software development tools enabling integration of complex systems.
- **Service Level Agreements:** Contracts outlining service expectations, crucial in vendor-client relationships.
- **Spoofing:** the act of falsifying data to gain unauthorized access.
- **Synthetic Identity Attack:** Creating a new identity using combined real and fake information.
- **Textual Verification:** ID number lookup or matching against ID authority database.