ENTRUST CYBERSECURITY INSTITUTE PRESENTS

Identity Fraud Report 2024

ENTRUST

SECURING A WORLD IN MOTION

Contents

Securing our digital future with AI-powered identity-centric security

Foreword

In today's environment — where much of how we interact, work and conduct business is digital-first — everything from business security to data protection, to user privacy are increasingly under threat.

Looking to the future, enhanced cybersecurity and fraud prevention are essential to build a foundation of trust for our collective digital future.

Nowhere is that foundation of trust more important than at the onboarding stage as part of digital account openings. From day one, businesses need to trust that customers are who they say they are and keep fraudsters off their platforms. On the flip side, customers need to trust a business is taking adequate steps to secure their data and protect them from fraud.

The methods used to verify identities and build trust at onboarding form the basis of secure interactions across the whole account lifecycle — from account opening, to account recovery, to account close. Trust built on day one extends across day 10, day 100, and beyond, giving businesses the best chance of minimizing the impact of fraud throughout the customer lifecycle.

This report shares the unique fraud trends businesses see during that key moment of onboarding, and offers insights on how to tackle them. Below is a summary of how the key trends from 2023 have developed in the last six months since this report was published*.

1. Digital forgeries continue to increase:
Last year, digital forgeries accounted for 16.7% of all document fraud attempts. In the last six months, that figure has doubled — 34.8% of all document fraud attempts now include some form of digital manipulation. A lot of this can be attributed to the emergence of websites such as OnlyFakes; an online service that sells the ability to create images of identity documents it claims are generated using AI.
At this time, the OnlyFake site has gone down, however, businesses should be aware of similar threats that fraudsters will try to capitalize on.

2. Fraud is, once again, becoming more difficult to catch:
The last few years saw a shift to less sophisticated fraud, with fraudsters favoring volume over sophistication. In 2023, 80.3% of all fraud Onfido caught was classified as 'easy' (lower sophistication). However, in the last six months, there has been a rise in both 'medium' and 'hard fraud. 36.4% of fraudulent attempts in the last six months were classed as 'medium' (up from 19.6% in 2023) and 1.4% as 'hard' (up from 0.1% in 2023). This is linked to the increase in digital forgeries, which can be harder to detect visually.

3. Deepfakes are here to stay:
The volume of deepfake attempts increased dramatically between 2022 and 2023 (3,000%). In 2022, it was rare to see fraudsters using deepfakes to attempt to bypass biometric verification at onboarding. In 2023, that all changed. The volume of deepfake attempts rose dramatically, accounting for the 3,000% increase. Due to the increasing availability of deepfake software and improvements in AI, their volume and sophistication will likely increase in 2024. In the last six months, deepfakes have accounted for roughly 30-40% of all biometric fraud Onfido catches. Currently, it's a small number of fraudsters who are responsible for creating deepfakes at scale, and this same group of fraudsters is attacking different customers using the same methods. But given fraudsters are inclined to resell or share their tactics with other fraudsters, this could change.

It's never been easier or cheaper to be a fraudster. Sites like OnlyFake, the availability of deepfake software, and the mass of personal data available on the dark web mean more fraudsters have access to increasingly sophisticated means of attack. Today, fraudsters are often organized, criminal enterprises that operate like businesses. Fraud and cybersecurity attempts have shifted from opportunistic, one-off attempts to targeted, scalable attacks. Time and again, fraudsters continue to adapt their methods to attempt to bypass security systems. In the face of these threats, securing our collective digital future for businesses and consumers alike is of utmost priority.

About Entrust

At Entrust, we work with our customers to protect data, enable strong identities, and secure payments across a variety of industries, including financial services, government and enterprise.

By acquiring Onfido — who have prevented approximately $6 billion in potential fraud for their customers in the last 18 months — Entrust can now combine AI-powered biometrics and global Identity Verification with Identity & Access Management in an integrated solution to fight deepfakes, phishing, account takeover (ATO) attacks and other threats. Onfido's AI is specifically designed to identify and stop these types of attacks. Trained and tested by an in-house Fraud Lab, unique micro-model architecture combines over 10,000 machine learning models trained to detect specific fraud markers, detecting up to 50% more fraud than approaches using generalized models.

Digital onboarding for financial services and payments starts with real identity, verifying the person and their credentials. Financial services and payments companies will now be able to onboard trusted customers, authenticate them, and issue debit cards in a matter of minutes while reducing their fraud exposure and remaining compliant with international regulations and standards. In the Identity Access Management (IAM) space, Entrust will integrate Onfido's AI-powered tools into its existing IAM solutions to protect critical assets and transactions with enhanced authentication, leveraging biometrics and digital certificates.

*The data referenced here is from the last 6 months, 1 September 2023-1 March 2024. The data analyzed in the rest of this report spans the previous year, 1 September 2022-1 September 2023.

Executive summary

An introduction to fraud

Welcome to this year's edition of Onfido's annual Identity Fraud Report. Every year we examine our proprietary data to identify emerging fraud trends, patterns, and techniques to help businesses keep fraudsters out from day one.

As an identity verification provider, we have a unique insight into how fraudsters target an integral part of the customer journey — onboarding. This first moment of interaction, combined with the know-your-customer (KYC) process, is a business's primary opportunity for detecting and preventing fraud and financial crime.

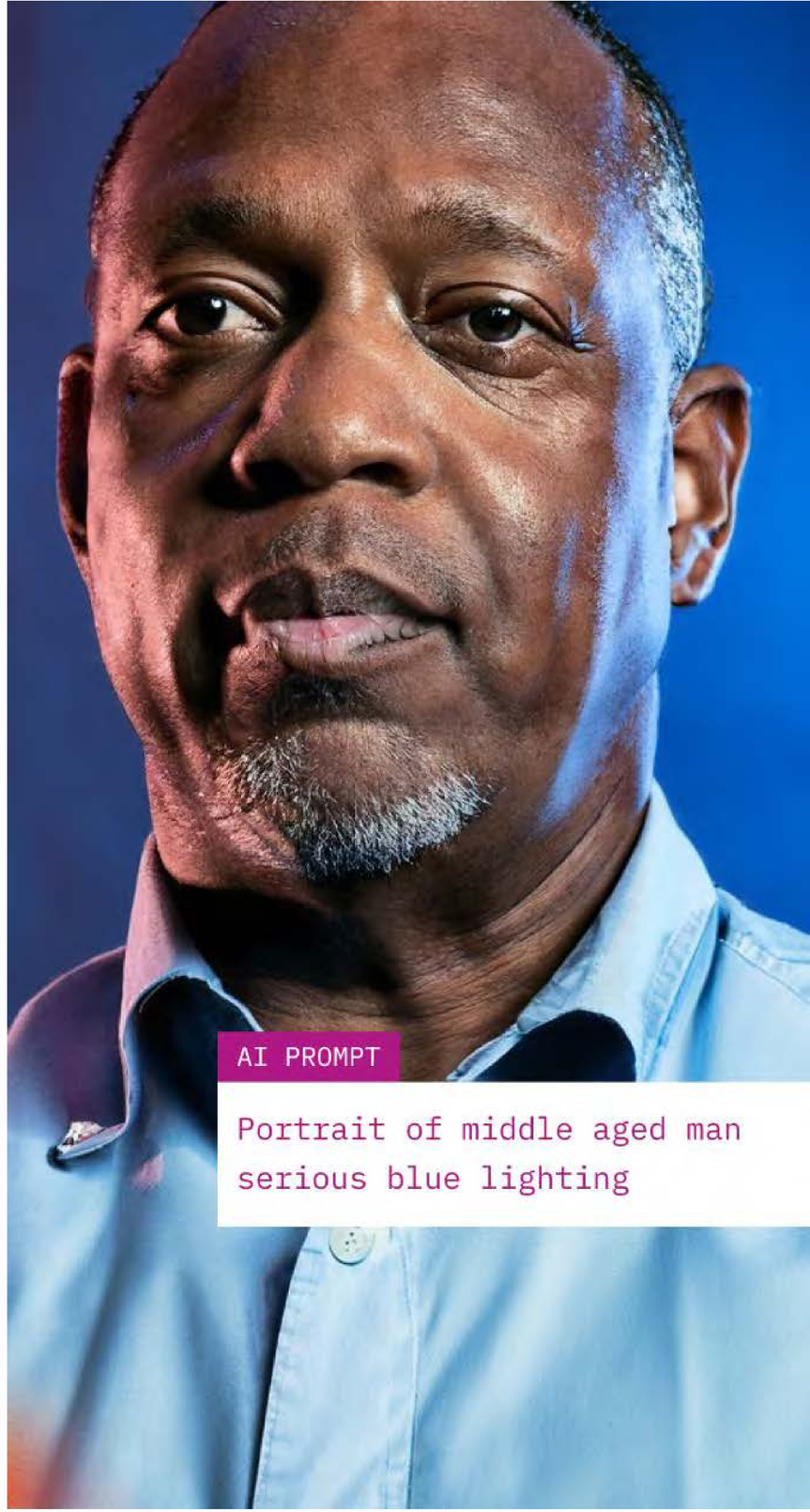
Identity verification helps to do this through a series of checks, including document verification, biometric verification, data validation, and fraud detection signals. It's by analyzing the fraudulent attempts we see across these checks that we can build a better picture of general identity fraud trends.

About our data analysis

The data analyzed in this report is taken from 1 September 2022 — 1 September 2023. In some cases, we compare this data to previous years to get a better and more accurate understanding of the overall trends. The data and trends are reflective of the verification space, and might not always mirror wider market trends. Onfido obtains the right to publish this data.

About our imagery

All human imagery in this report was created with the help of AI, and refined by Onfido's team of designers. We chose to create the imagery in this way to highlight the progression of deepfakes and how AI is infiltrating many different elements of our lives.



A note from our fraud experts

Key themes from this year's report

It's been five years since we released our first annual Fraud Report, and five years marks a milestone in identity fraud analysis. So I wanted to take some time to reflect on the changing fraud landscape and the latest emerging threats.

1. Document manipulation is increasing

A big theme we're seeing emerge from this year's data is that the availability of online tools and improved AI tooling are opening up new avenues for fraudsters. This is true across documents, as well as biometrics. While physical counterfeits still account for the majority of fraud cases, there is a notable swing towards digitally altering smaller areas of a document, whether it be partial or total face swaps, or changing just a few of the details. Improved AI tooling and the availability of online tools make this a more scalable option.

2. Biometric fraud is developing, fast

Biometric verification is still one of the most secure ways to detect and prevent fraudulent attempts. However, as biometrics have become more widely adopted as a means of defense, fraudsters are starting to become more creative in their means of attack. Average biometric fraud rates in 2023 are 2X what they were in 2022. Businesses and identity verification providers alike should leverage the latest defense models, including verification that incorporates AI and liveness.

3. Fraudsters go digital with deepfakes

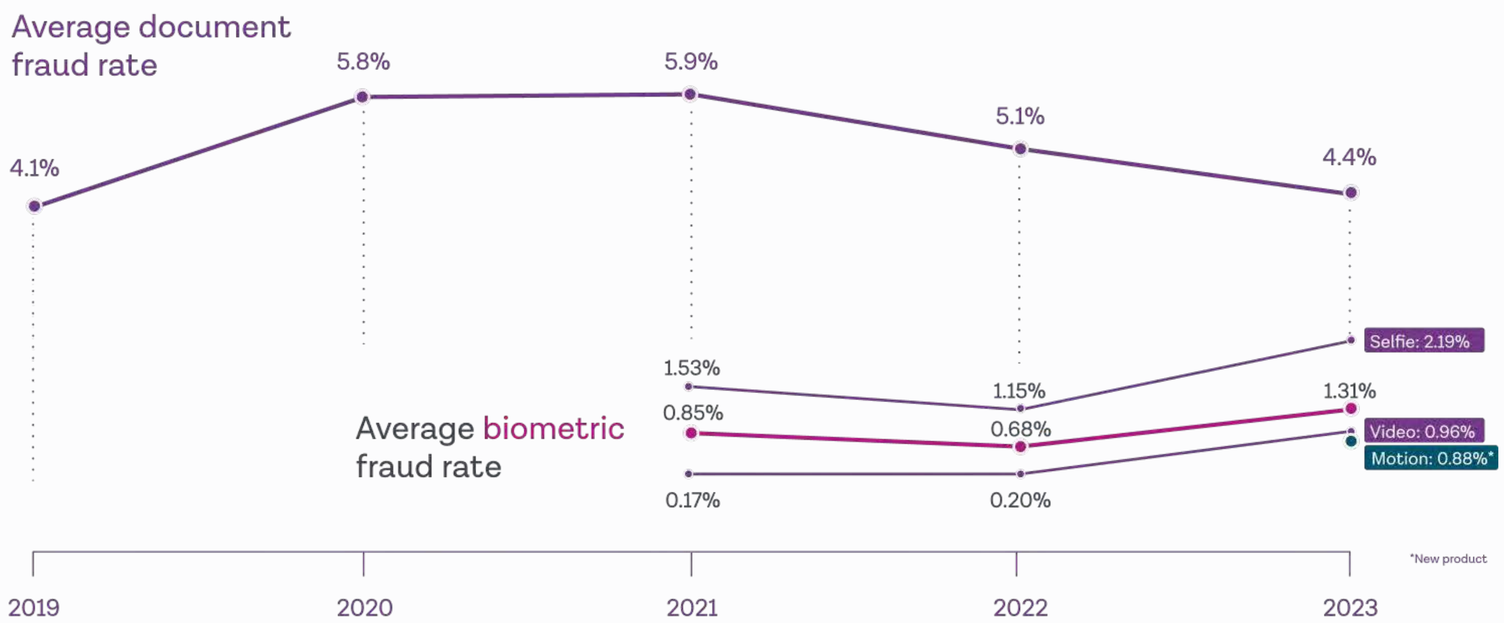
One way fraudsters are getting creative with biometric fraud is with deepfakes. The availability of online tools and generative AI, such as face-swapping apps, are aiding fraudsters in their pursuits. There has been a 31X increase in the volume of deepfake attempts in 2023 compared to 2022. One way businesses can counter deepfakes is to leverage liveness biometric verification technology, such as Onfido Motion, powered by deep learning anti-spoofing AI models.

Fraud at a glance

The big picture and trends

Average fraud rates point to the volume of fraudulent activity. In other words, where fraudsters are focusing their efforts. Comparing the data year-on-year points to wider trends across the identity fraud landscape.

Average fraud rates



This year's data suggests fraudsters are starting to place more emphasis on biometric fraud. Document fraud rates continue to follow a consistent trend. After peaking in 2021, they have leveled out over the last few years, averaging 4.4% in 2023.

Comparatively, there's been a slight uptick in biometric fraud in the last year. The 2023 average biometric rate (1.31%) is 2X what it was in 2022 (0.68%). Increasingly, fraudsters use a genuine document (obtained via a data leak) for the document verification check, and then change their face for the biometric check.

This reinforces another emerging trend — fraudsters are turning to techniques like cheapfakes and deepfakes as a means of attack across biometrics.

But biometrics still see markedly less fraud compared to documents — roughly 3X less. This shows biometrics continue to act as an effective deterrent, particularly solutions with a liveness element. Onfido's Video and Motion products in particular prove a good deterrence for fraud, with rates below 1%.

01

Decoding document fraud

Decoding document fraud

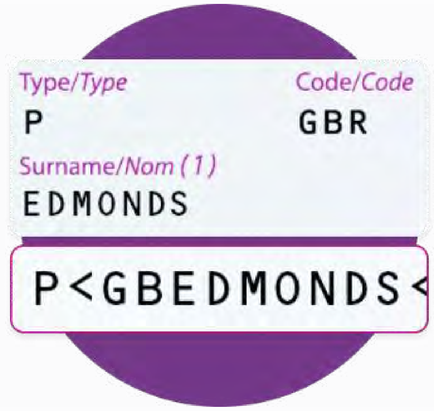
How do fraudsters target identity documents?

Fraudsters use different combinations to try and bypass security. For example, they might use a fake document combined with their own face, or vice versa. Or they might tamper with both the document and the biometric element.

Document verification is the first line of defense against identity fraud. It involves analyzing digitally submitted images of documents for signs of fraud, including:

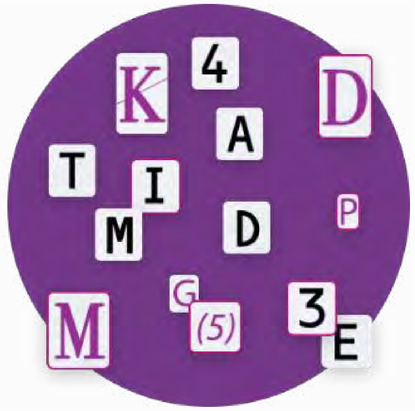
Photos

Pictures should be the correct color, or black and white depending on the document type, and the secondary portrait should match the primary picture.



Data

The information contained in the MRZ (machine readable zone) should reflect the data within the document.



Fonts

Different documents (and areas of the document) use different types of fonts. An incorrect font could be a sign of fraud.

From physical to digital document manipulation

Fraudulent documents fall into one of two categories:

Counterfeit
A complete reproduction of an original document

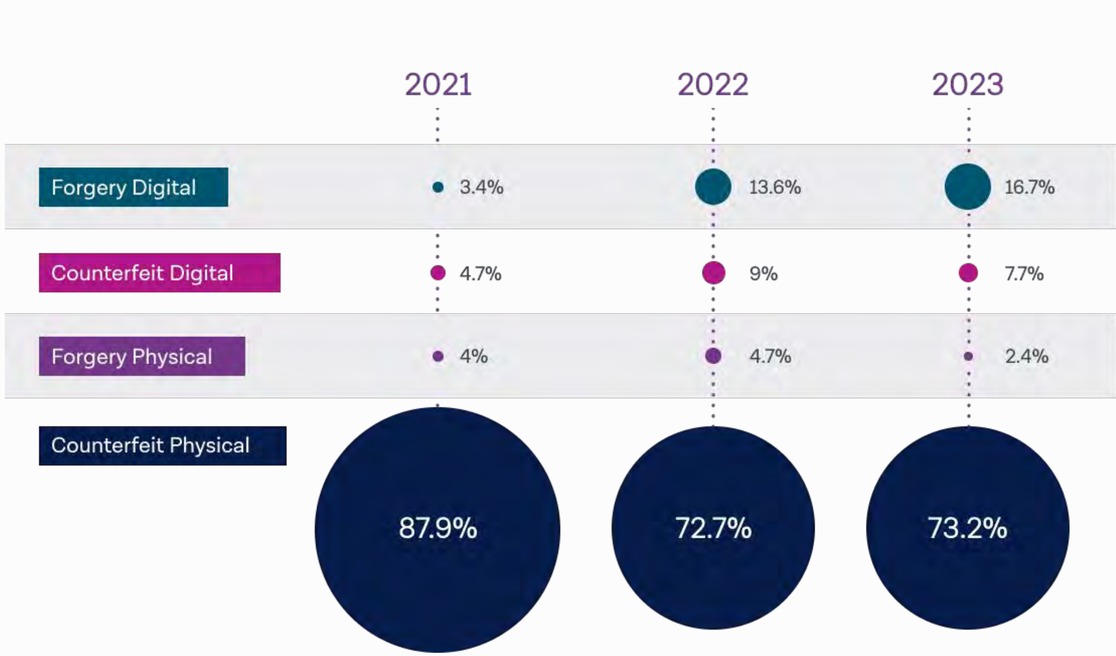
Forgery
An altered version of an original document

And fraudsters use one of two methods when defrauding documents:

Physical
Fraudsters create or edit a physical document, then submit a photo of it

Digital
Fraudsters create or alter a digital representation of a document using digital tools

How fraudsters target documents



Counterfeit

Forgery

This data highlights that fraudsters prefer to start from scratch when creating fake physical documents.

However, they are more inclined to use an existing template (for example an image of a document found online) when digitally manipulating documents.

Physical counterfeits still account for the majority of document fraud (73.2%). This is partly due to the fact that the majority of Onfido's customers use our SDKs. These SDKs require users to capture an image of their document live, which makes it much harder for fraudsters to submit digitally modified images.

However, there has been an 18% increase in digital forgeries over the last year (and roughly 5x more digital forgeries in 2023 compared to 2021). This trend is likely to continue because digitally manipulated images are quicker and cheaper to produce than physical fake documents, especially given the increased availability of AI tooling.

Easy pickings: Why fraudsters opt for scalable attacks

Examining fraud sophistication helps determine what types of attacks fraudsters favor. Are they creating a small number of high-quality fakes, or do they prefer to try and brute force a business's defenses?

Most of the document fraud from 2023 (80.3%) is 'easy'. This means that the errors on the document are visible to the trained eye.

A note from the experts

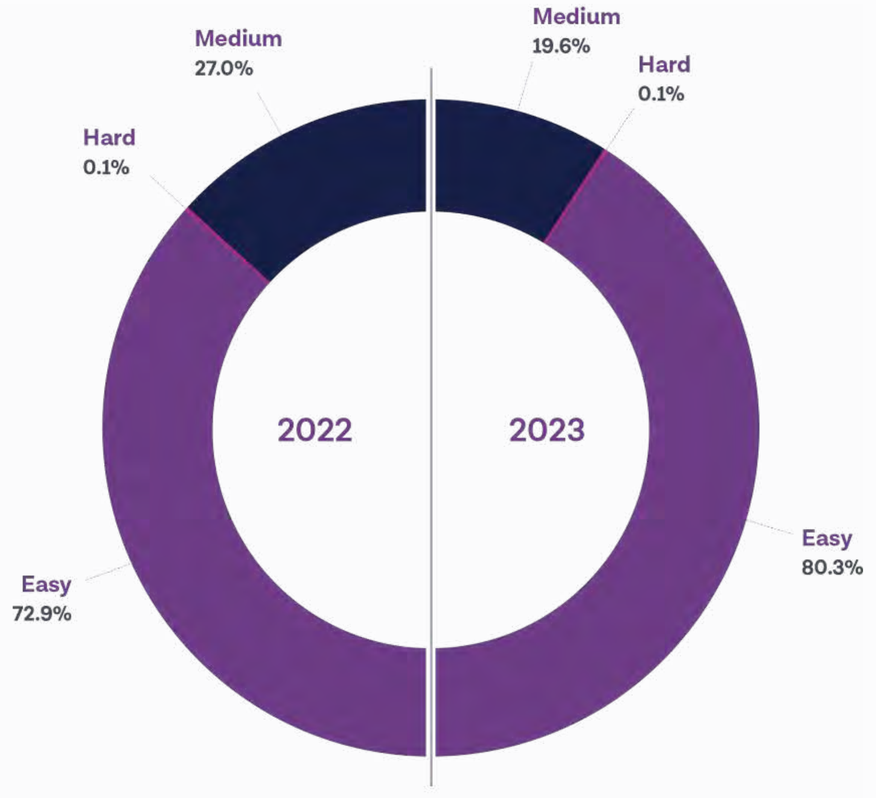
This points to a long-standing trend we know about fraudsters.

They are looking for minimum effort, maximum reward results, and do so by attacking in volume.

By using scalable models to attack businesses, they are able to determine what sticks before using that loophole to attack en masse.

Businesses should respond by having a scalable, automated fraud detection system in place, to catch these large-scale attacks.

Fraud sophistication



Easy

Document elements are clearly wrong and visible to the trained eye. For example, an obviously manipulated photo.

Medium

Less obvious errors that require some skill to detect. For example, the wrong printing technique.

Hard

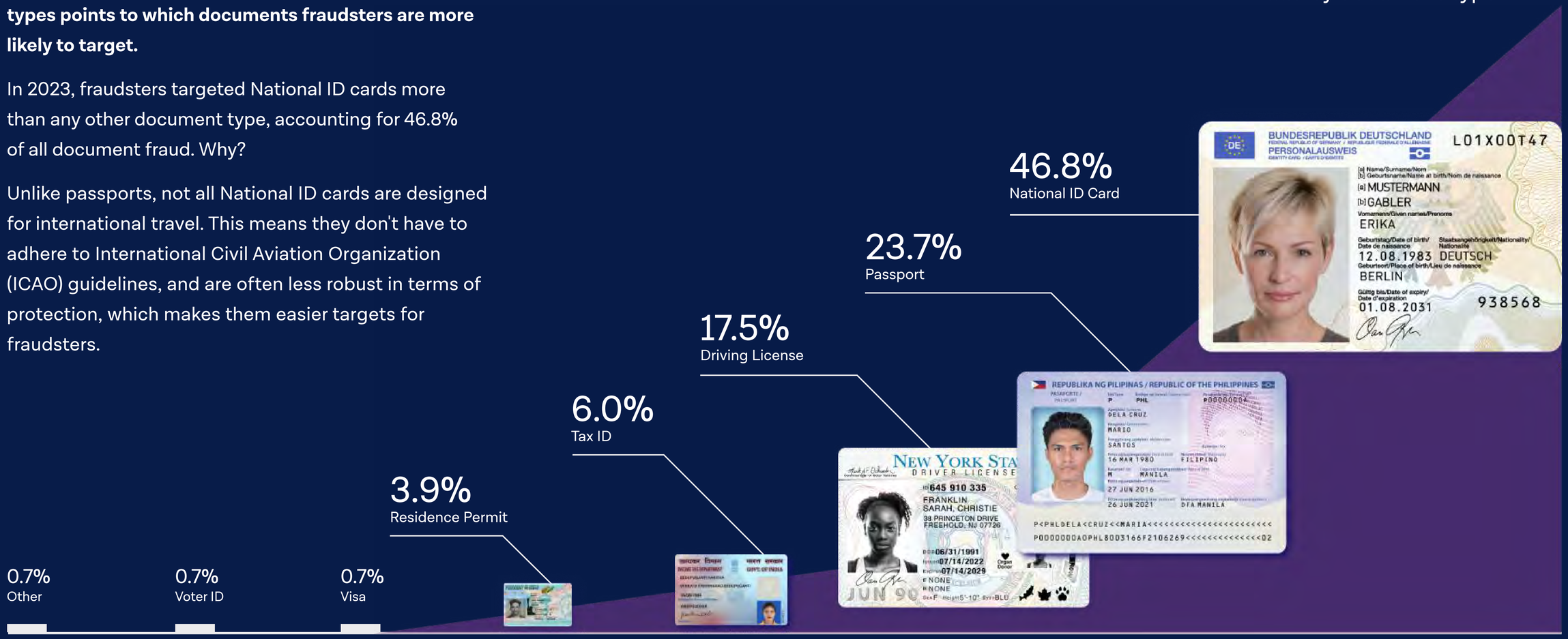
Errors that would require enhanced knowledge of document manufacturing to detect.

Fraudster preferences: A renewed focus on National ID cards

Examining the fraud rate across different document types points to which documents fraudsters are more likely to target.

In 2023, fraudsters targeted National ID cards more than any other document type, accounting for 46.8% of all document fraud. Why?

Unlike passports, not all National ID cards are designed for international travel. This means they don't have to adhere to International Civil Aviation Organization (ICAO) guidelines, and are often less robust in terms of protection, which makes them easier targets for fraudsters.



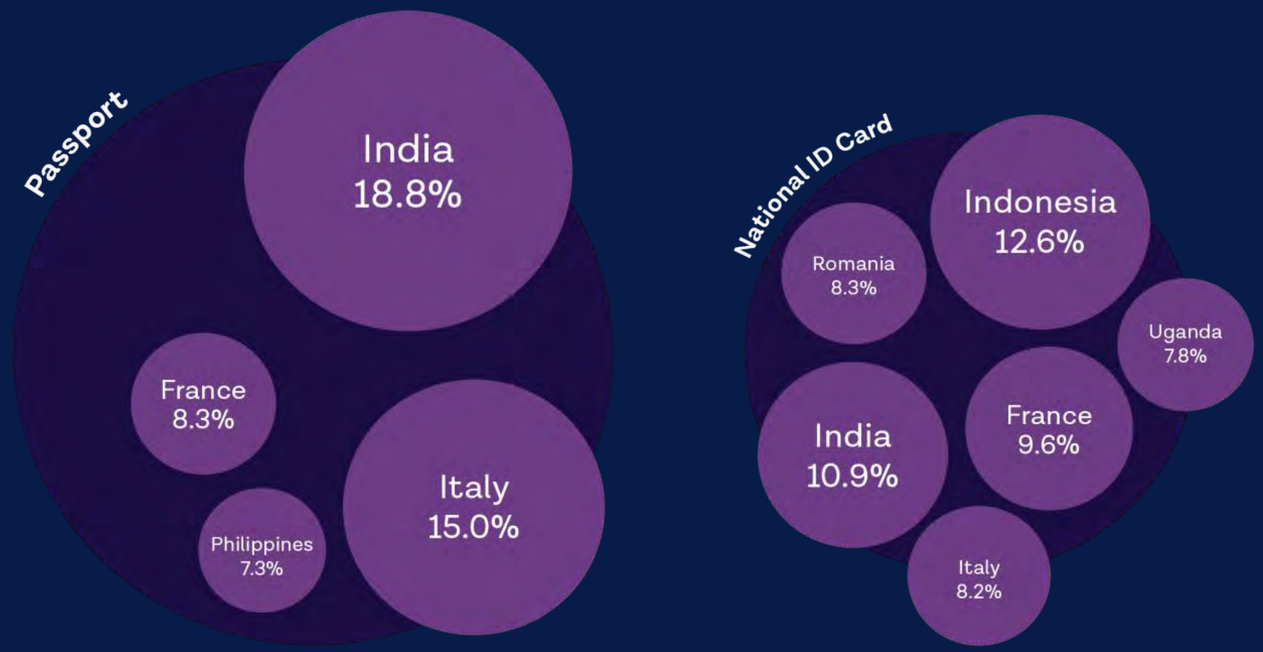
Fraudsters' favorites: The 10 most targeted documents

National ID cards also feature heavily on the list of most targeted documents. There are many reasons why fraudsters target one type of document over another.

Several of the documents that feature in this list still have older versions of the document in circulation. Generally (although not always) older documents have fewer security features and are less secure. When documents have been in circulation for a long time, fraudsters tend to become familiar with how to attack them, and exploit this.

A lot of the documents that feature on this top 10 list are also the most common form of identification in that country. This means getting hold of templates or fake versions of these identity documents is probably easier.

Suspected fraud (%)



Passport, India	18.8%
Passport, Italy	15.0%
National Identity Card, Indonesia	12.6%
National Identity Card, India	10.9%
National Identity Card, France	9.6%

National Identity Card, Romania	8.3%
Passport, France	8.3%
National Identity Card, Italy	8.2%
National Identity Card, Uganda	7.8%
Passport, Philippines	7.3%

02

Breaking down biometric fraud

Why biometrics?

Rising threats, stronger defenses

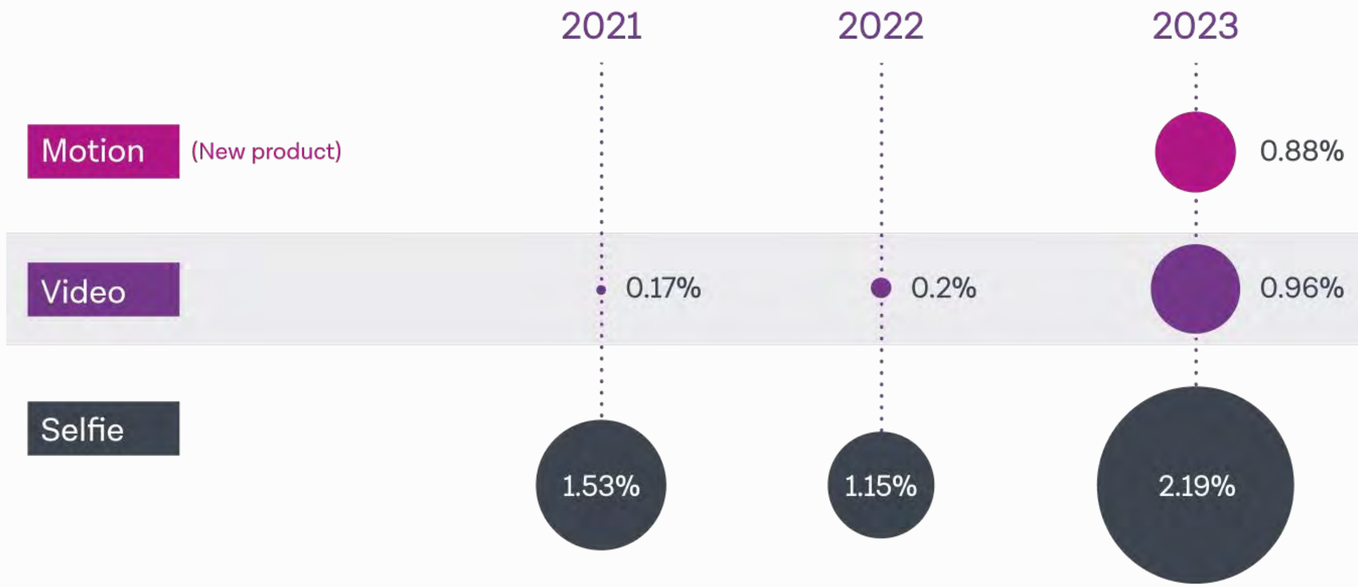
As identity providers and businesses alike have put in place stronger defenses, fraudsters are trying to find new, more innovative ways to get around security. The influx of readily available online AI-assisted tools, such as face-swapping apps, has also given fraudsters a new avenue into biometric fraud.

This is clear from the data. Biometric fraud attempts are higher in 2023 than they've been in previous years.

The message is clear. Rising threats need stronger defenses. Biometric verification offers an extra layer of protection on top of document verification. Matching a facial biometric to a photo ID helps determine:

1. There is a real person attempting to sign up for a service, and
2. That the identity document belongs to the person presenting it.

Average biometric fraud rates



In response to increasingly sophisticated biometric fraud techniques, such as deepfakes, Onfido launched Motion — a fully automated biometric solution that simply requires users to turn their heads as part of a video capture. Motion uses advanced liveness and anti-spoofing technology to offer a seamless user experience, while protecting against emerging fraud vectors such as deepfakes and injection attacks. It's proven to deliver a 10X anti-spoofing performance improvement with 95% of checks returned in <15 seconds.

A note from the experts

The message is clear. Rising threats need stronger defenses. Biometric verification offers an extra layer of protection on top of document verification. Matching a facial biometric to a photo ID helps determine that:

1. There is a real person attempting to sign up for a service, and

2. That the identity document belongs to the person presenting it.

Screens and spoofs: How fraudsters target biometrics

Fraudsters most commonly target Selfie biometric checks using one of the following methods:

1. **Taking a photo of a different face on a screen** (such as a profile picture from social media accounts) as opposed to using their own face.

2. **Taking a photo of the photo on the document** and trying to pass that off as a biometric, instead of a real face.

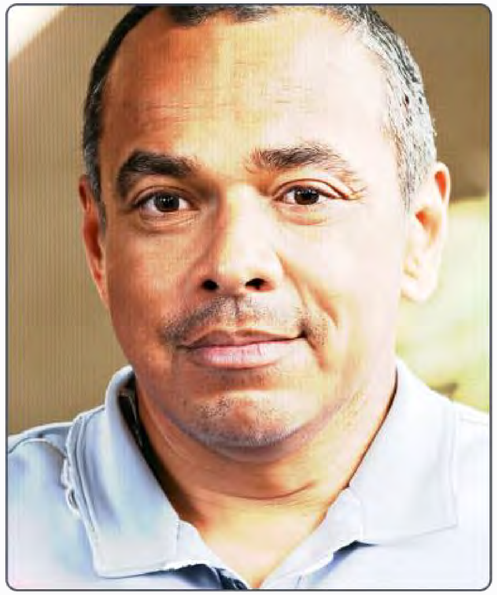


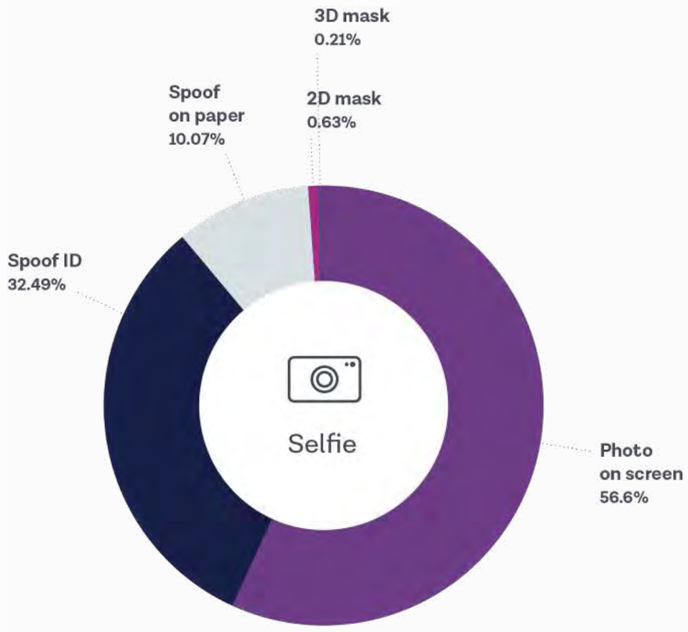
Photo of a different face on a screen

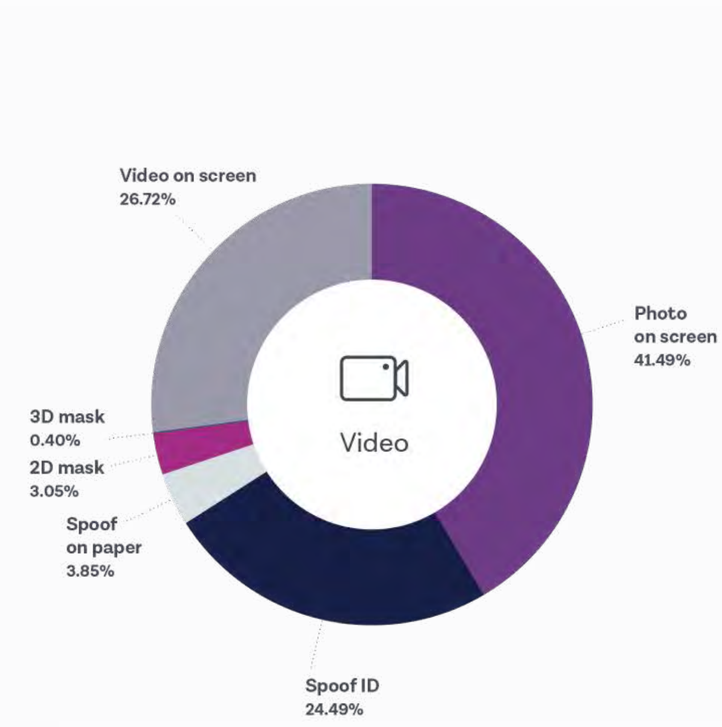
AI Prompt: Portrait of middle aged man looking at camera

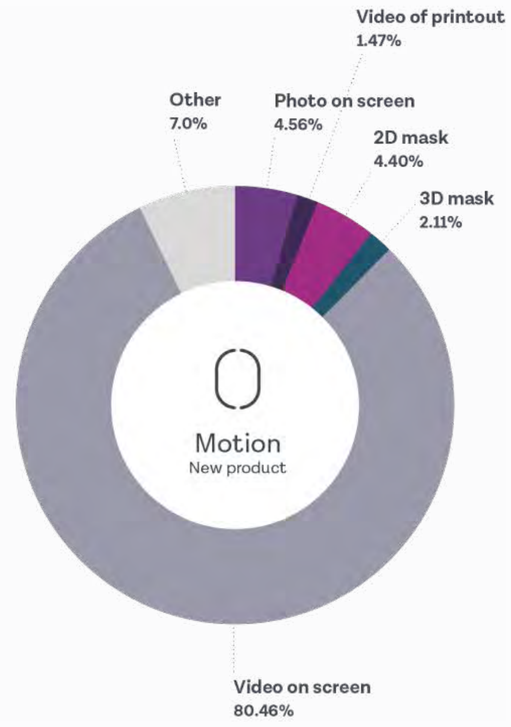
Photo of the photo on a document

AI Prompt: Caucasian blonde woman serious looking straight at camera white background black and white

Types of biometric fraud







Across Video and Motion, the biggest attack vectors are photos on screen or videos on screen.

This points to techniques such as cheapfakes and deepfakes, where fraudsters use digital manipulation tools to edit their face during a video capture.

Key

Photo on screen
A photo or video of an image on screen

Spoof ID
A photo or video of the image on the identity document

Spoof printed on paper
A photo or video of an image printed on paper

2D mask
A photo or video of a 2D-printed mask

3D mask
A photo or video of a 3D mask or other 3D object

Video on screen (Video/Motion only)
A video of a video on screen

Video of a face or image printed on paper

Other

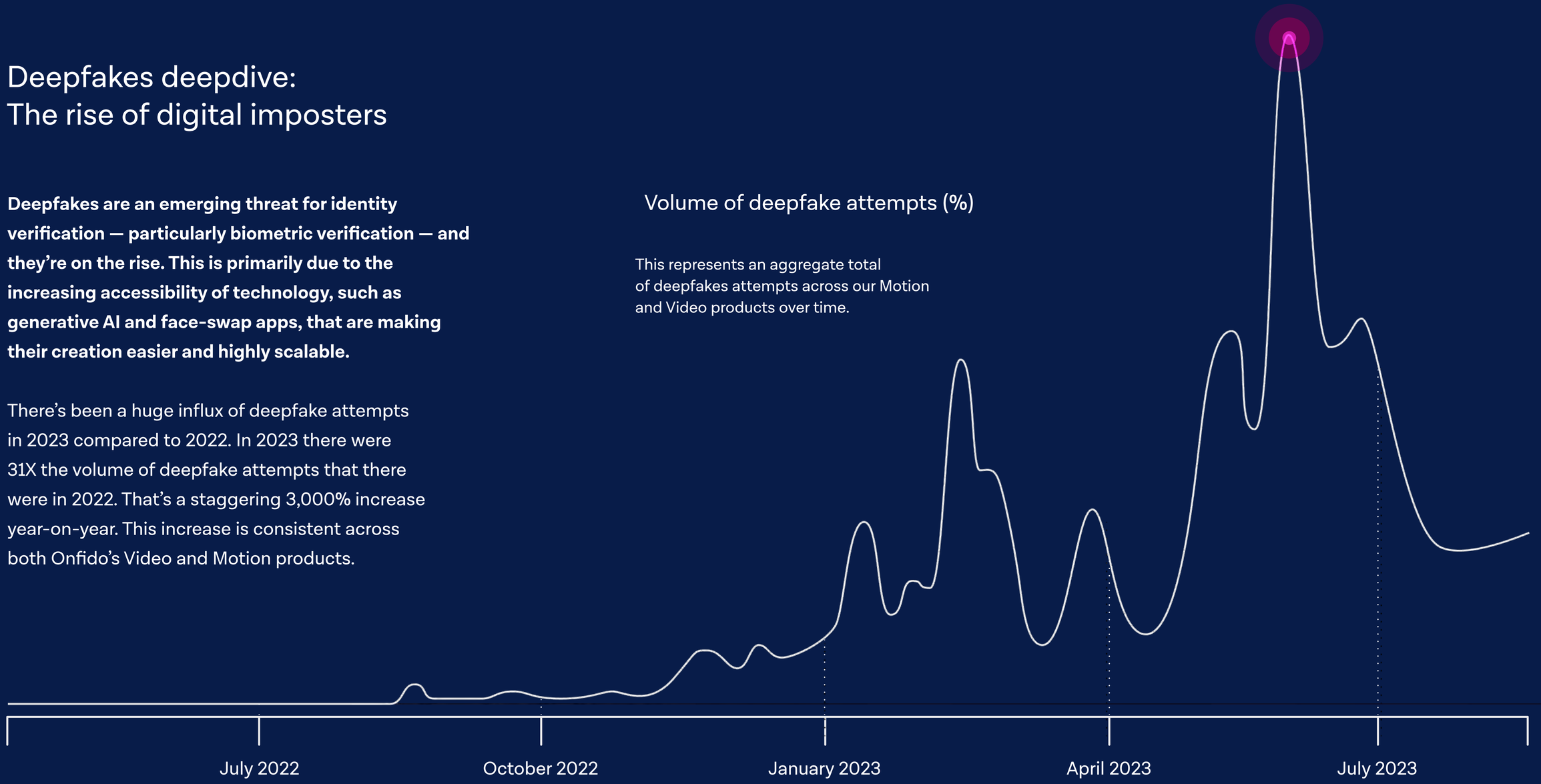
Deepfakes deepdive: The rise of digital imposters

Deepfakes are an emerging threat for identity verification — particularly biometric verification — and they're on the rise. This is primarily due to the increasing accessibility of technology, such as generative AI and face-swap apps, that are making their creation easier and highly scalable.

There's been a huge influx of deepfake attempts in 2023 compared to 2022. In 2023 there were 31X the volume of deepfake attempts that there were in 2022. That's a staggering 3,000% increase year-on-year. This increase is consistent across both Onfido's Video and Motion products.

Volume of deepfake attempts (%)

This represents an aggregate total of deepfakes attempts across our Motion and Video products over time.



Facing up to deepfakes: What businesses need to know

What are deepfakes?

Deepfakes typically refer to digitally manipulated videos or images, where a person's face is altered to appear as someone else. It can be difficult to distinguish this fabricated content from genuine recordings or images.

Increasingly, fraudsters and cybercriminals are leveraging artificial intelligence (AI) and machine learning (ML) tools to create deepfakes and use them for malicious purposes.

Deepfakes vary in sophistication, and can fall into one of three categories:

Face swaps

AI Prompt: Man covering face with a paper print mask of a human face

In face-swapped images or videos a source face is superimposed onto a target head. The most basic way of doing this results in a 'cheapfake', where the source face is crudely pasted over the top of the target face. True deepfake face-swaps are much more sophisticated — they use AI to morph and blend the source face onto the target.

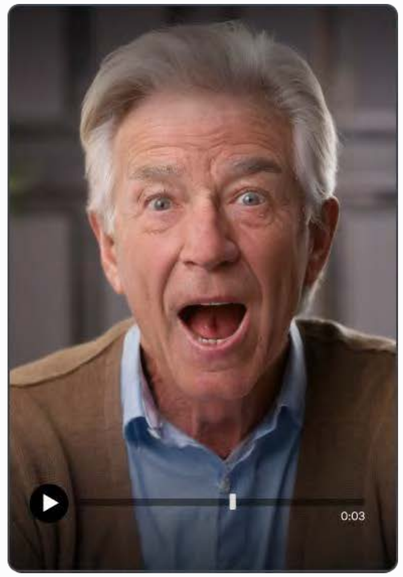
Fully-generated images

AI Prompt: Woman selfie portrait living room looking at camera blue hair tattoo

These are created by generative models that have been trained to produce extremely realistic images of faces.

In this scenario, a new face is produced entirely from scratch, rather than superimposing one face onto another.

Lip-sync videos



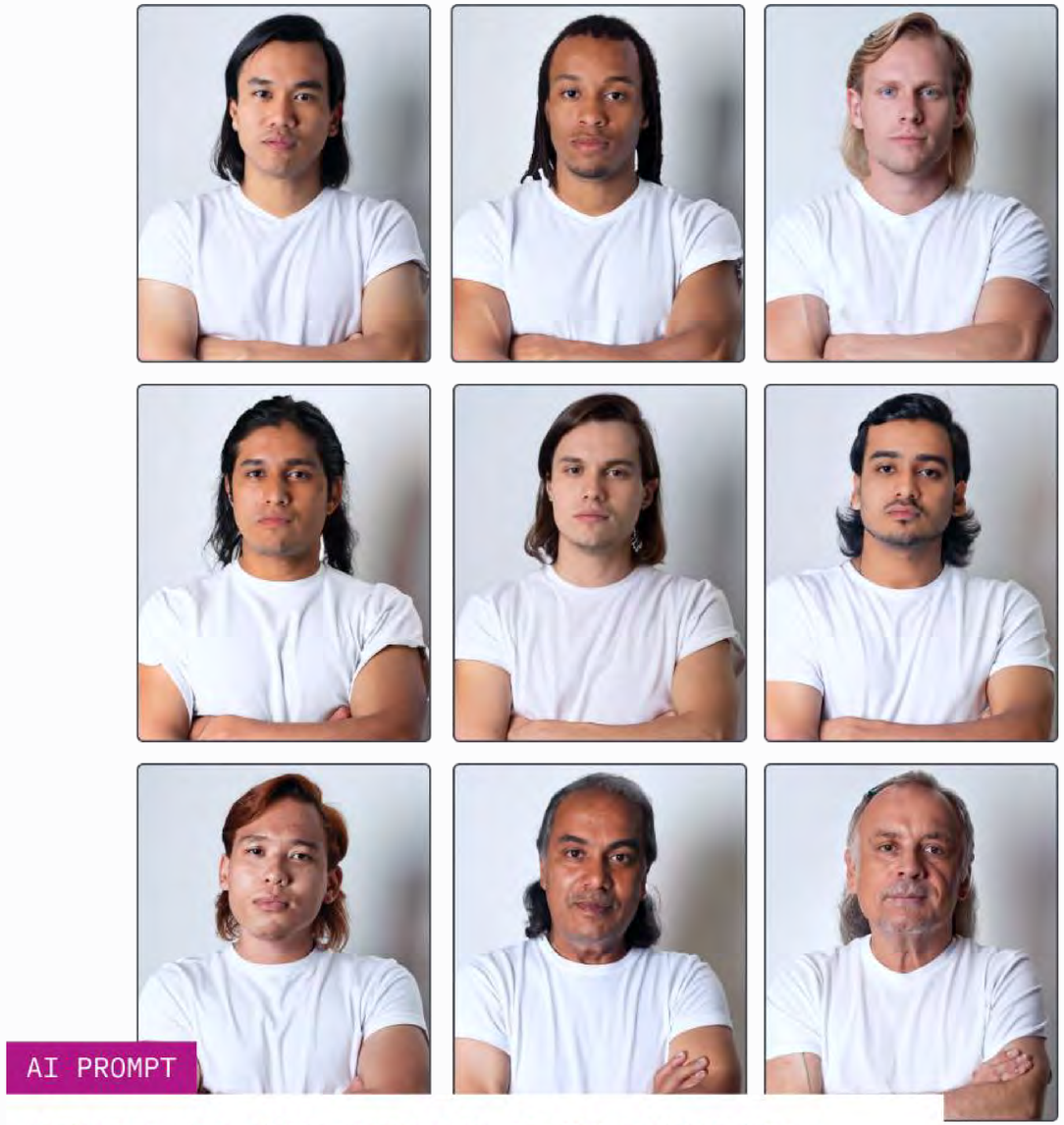
AI Prompt: older man talking looking at camera mouth half open

In these videos, the original person stays the same, but their lips are manipulated (and sometimes combined with deepfaked voices) to make it appear as though they are saying something they never said in the original video.

Key trends: How are deepfakes changing the fraud landscape?

Onfido has identified some key trends when it comes to how fraudsters use deepfakes:

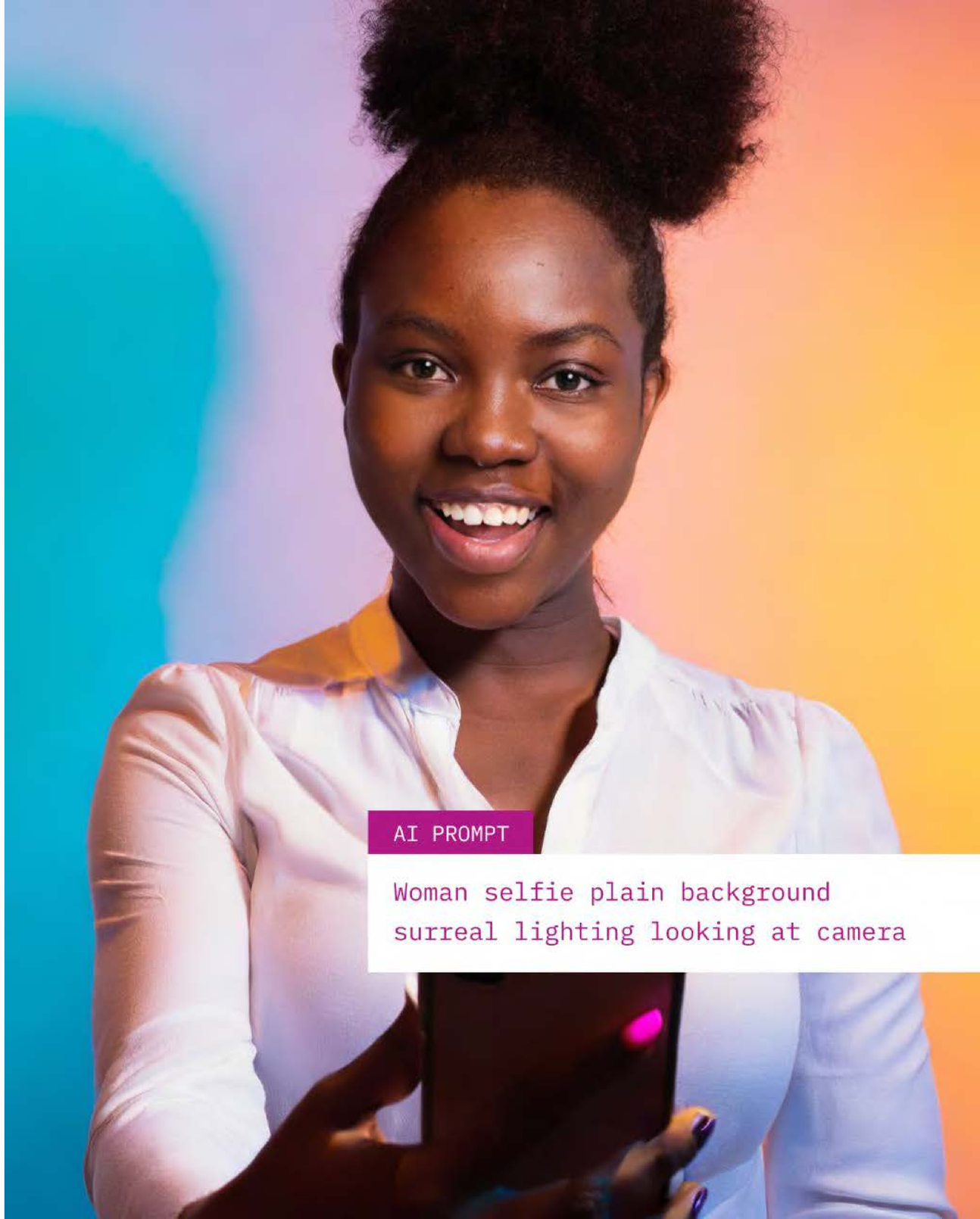
1. **A small number of fraudsters are responsible for the majority of deepfake attacks.** A single fraudster will submit tens or hundreds of deepfaked identities in a short space of time.
2. **Attackers tend to focus on a single business** (or small group of targets) at a time.
3. **Fraudsters use a variety of tools to create deepfakes**, including software they run themselves and online tools that provide deepfake creation for free or via paid subscription.



How to detect deepfakes

Detecting deepfakes requires a comprehensive approach that analyzes facial movements, expressions, voice, and audio characteristics. To have the best chance of preventing deepfakes, businesses should incorporate the following into their identity verification:

- **Fraud-detecting AI:** For example, Onfido uses our own in-house Fraud Lab to generate deepfakes, and then use these datasets to train our fraud-detection AI.
- **Liveness solutions:** Biometric products that check for liveness (for example, incorporating video or motion) make it harder for fraudsters to spoof the system while maintaining low friction for genuine users.
- **SDKs over APIs:** SDKs offer more protection than APIs. They have in-built fraud detection, such as live capture, which makes it much harder for fraudsters to upload digitally tampered submissions.
- **Cross-device workflows:** Deepfakes are typically more common on web browsers than SDKs. Enforcing cross-device verification can reduce the chances of pre-recorded videos, emulators, and fake webcams.



How does Onfido mitigate deepfakes?

Onfido's Biometric Verification offers enhanced deepfake protection by using a layered approach that aims to block deepfakes at the source. In other words, to proactively block deepfakes and prevent fraudsters from submitting them in the first place. We do this in a number of ways:

- **Making it harder for fraudsters to upload or bypass systems**, for example mitigating injection attacks.
- **Offering liveness solutions** (such as Motion and Video) which make it harder for fraudsters to craft deepfakes.
- **Improving and retraining the machine learning technology using generative AI.** Onfido's dedicated Applied Science team conducts regular reviews to identify new developments in fraud, such as deepfakes, and retrain our fraud detection models to react accordingly.

03

Timing is everything

Tick tock, fraudsters operate around the clock

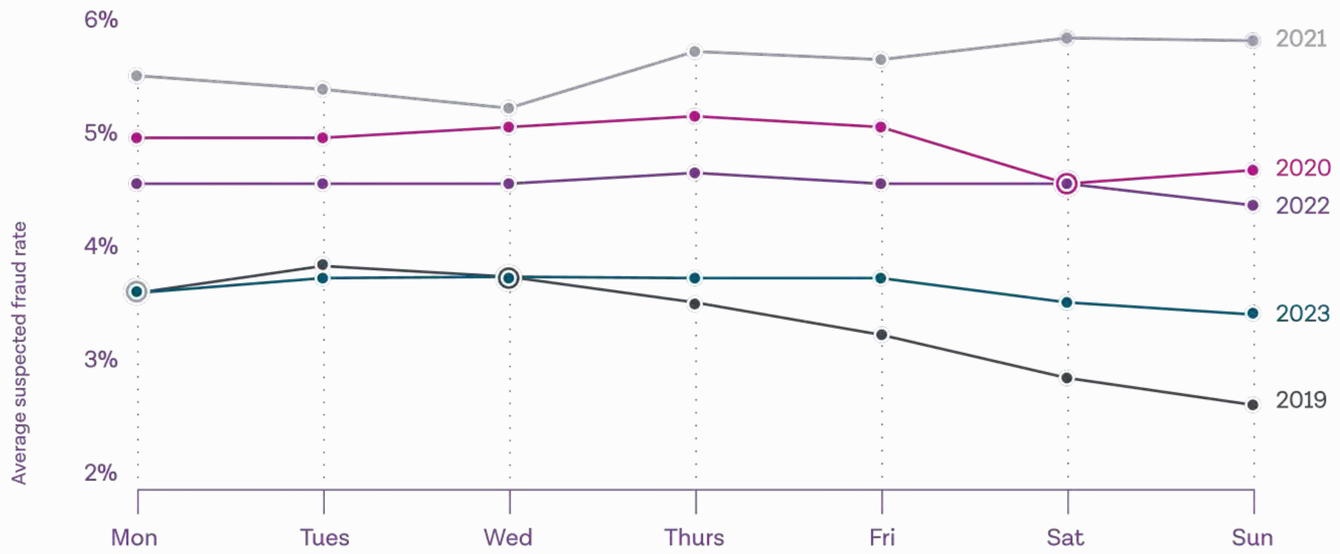
When are fraudsters most active?

When comparing data from the last few years, several patterns emerge that help determine when fraudsters are most active. While businesses should always be prepared for fraud, this analysis can help determine when future attacks are more likely to happen.

Over the last five years, there's been a clear shift in when fraudulent activity happens. Pre-COVID-19, fraudster activity mirrored an average working week, dropping at weekends. Peak pandemic, fraudulent activity spiked at weekends, suggesting fraud became more of a recreational add-on rather than a dedicated 9-5.

Over the last few years, fraud activity has been fairly consistent across all seven days of the week. This suggests fraud has become a global, interconnected activity, just like the way many modern businesses operate today.

Average fraud rates by day of the week

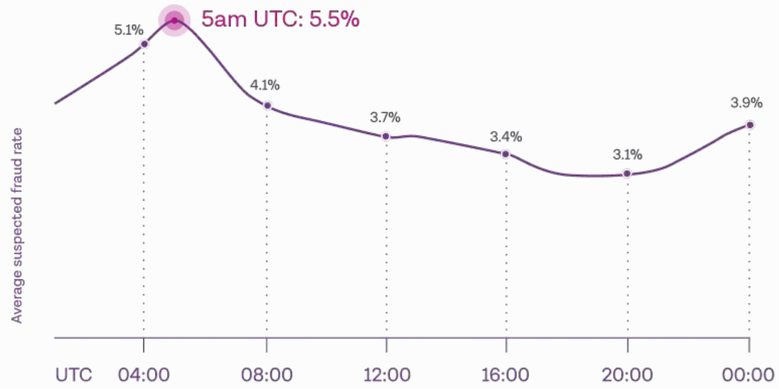


5am UTC: The fraud witching hour?

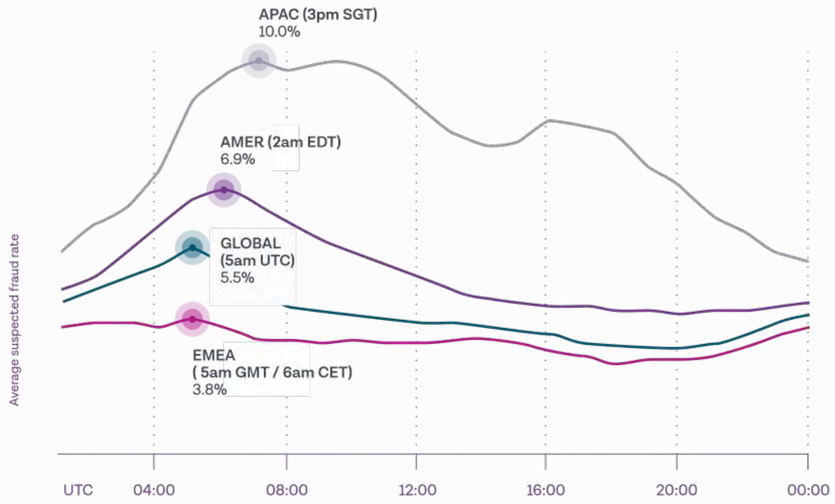
Fraud activity is also fairly consistent across all hours of the day, with the exception of one spike at around 5am UTC.

Interestingly, when examining this data from the perspective of different time zones, 5am UTM solidifies itself as ‘the fraud hour’. Regardless of where a business is based in the world, it seems they’re likely to see more fraud between the hours of 4 and 6am UTC.

Fraud level per hour, total



Fraud level per hour, per region



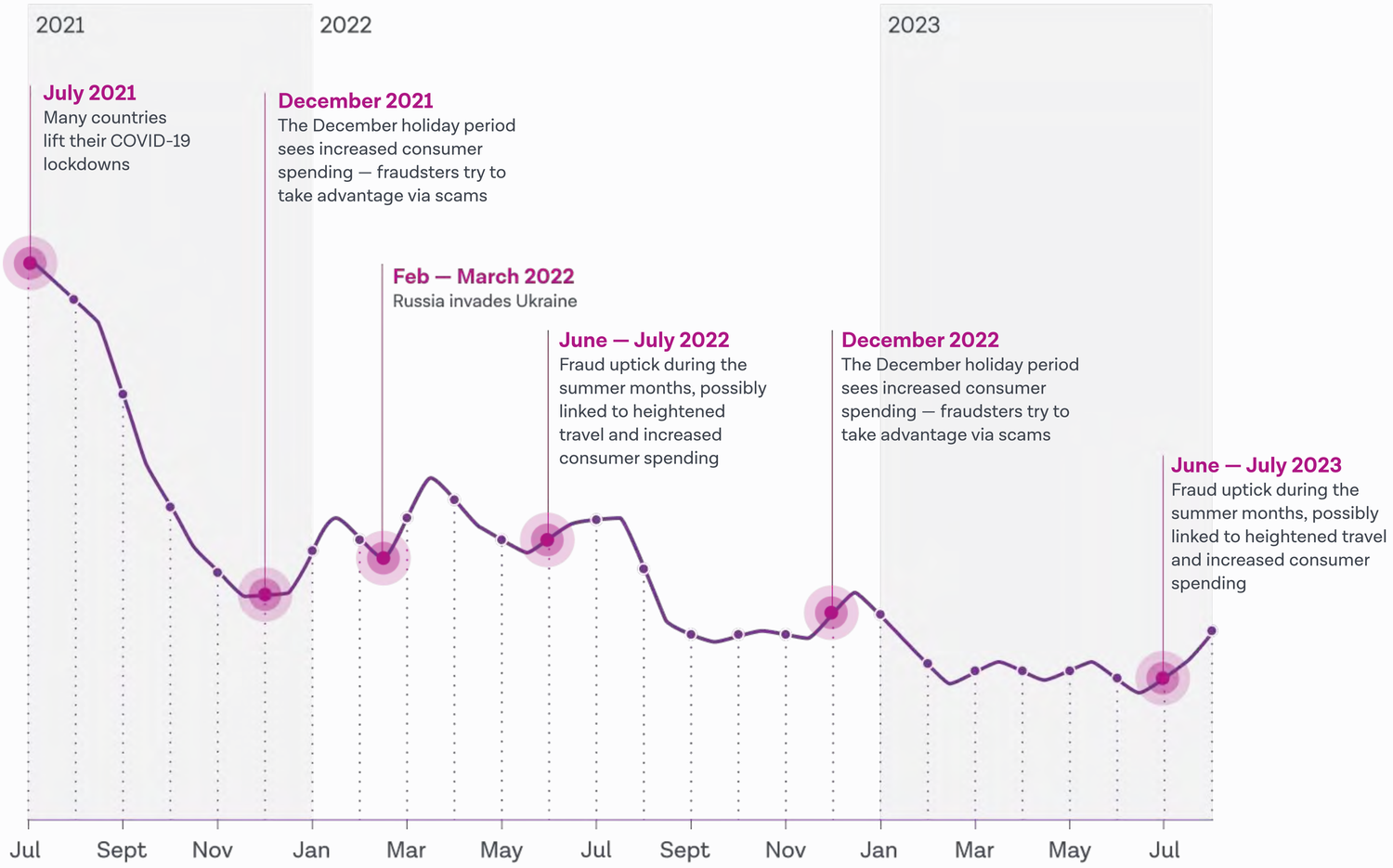
Yearly fluctuations: Navigating the rise and fall of fraud

Average fraud levels over the course of a year show several spikes. Firstly, fraud levels rise when they coincide with large-scale global events (such as when COVID-19 lockdowns lifted in summer 2021) or during periods of unrest (for example when Russia invaded Ukraine in 2022). Unrest, confusion, and financial insecurities can all lead to an increase in fraudulent activity.

The months of December and June-August often see a small spike in fraud. Fraudsters could be looking to take advantage of increased public spending during the holiday periods, or when international travel increases.

Businesses should take note of these yearly spikes, and the fraudster mentality that it reveals. Fraudsters follow the money or take advantage of unrest. So when it comes to a business's product offering, they should pay particular attention to potential fraud when running an introductory offer, sign-up bonus, or similar.

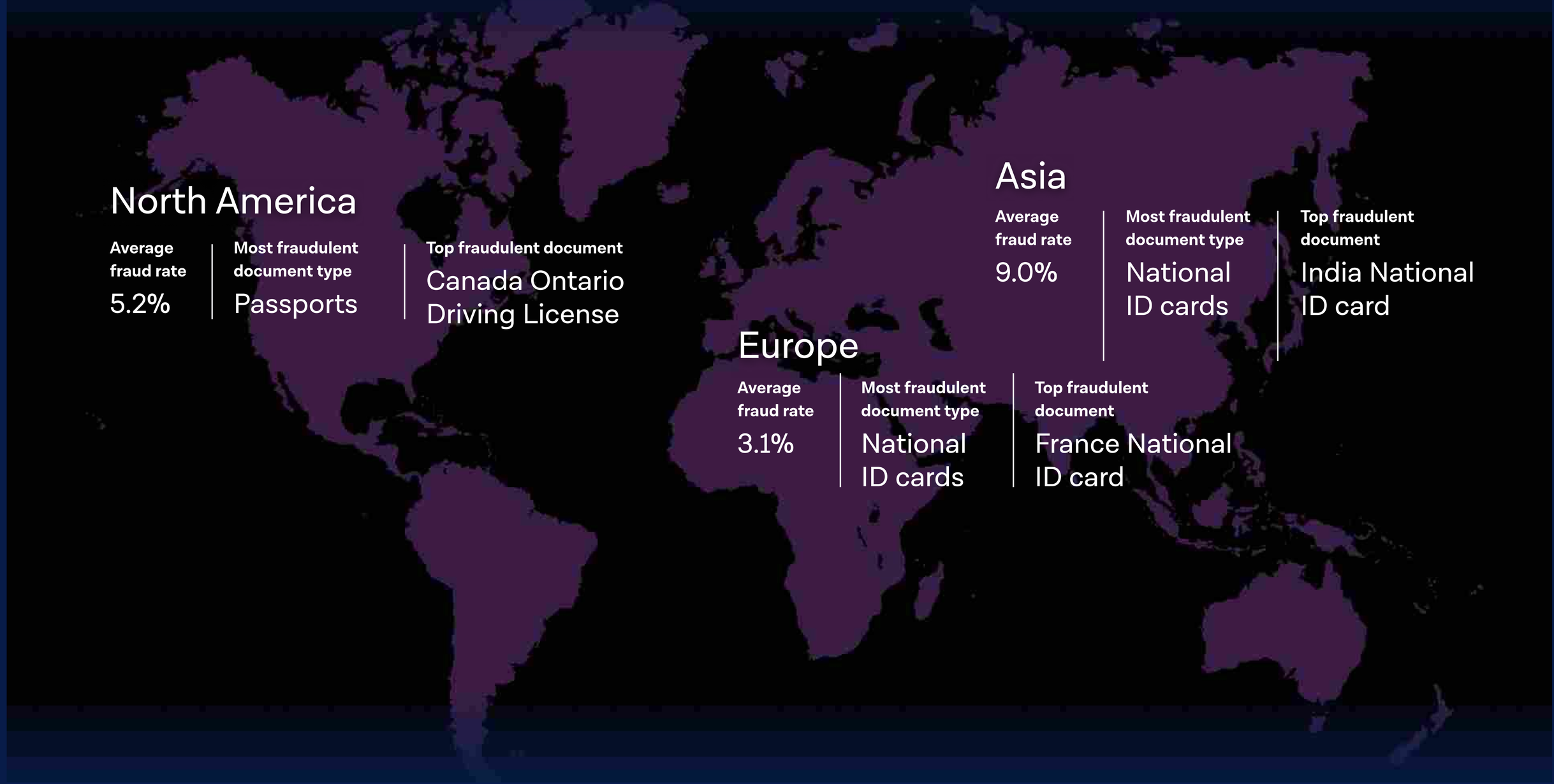
Months of the year fraudsters are most active



04

Fraud's global footprint

Where are fraudsters most active?



North America

Average fraud rate
5.2%

Most fraudulent document type
Passports

Top fraudulent document
Canada Ontario Driving License

Asia

Average fraud rate
9.0%

Most fraudulent document type
National ID cards

Top fraudulent document
India National ID card

Europe

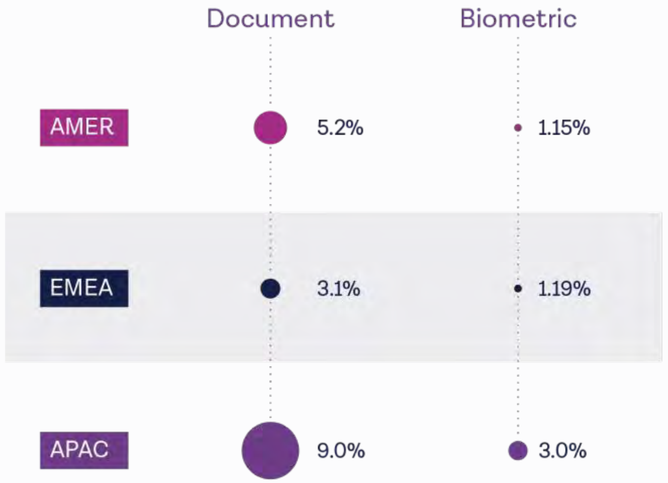
Average fraud rate
3.1%

Most fraudulent document type
National ID cards

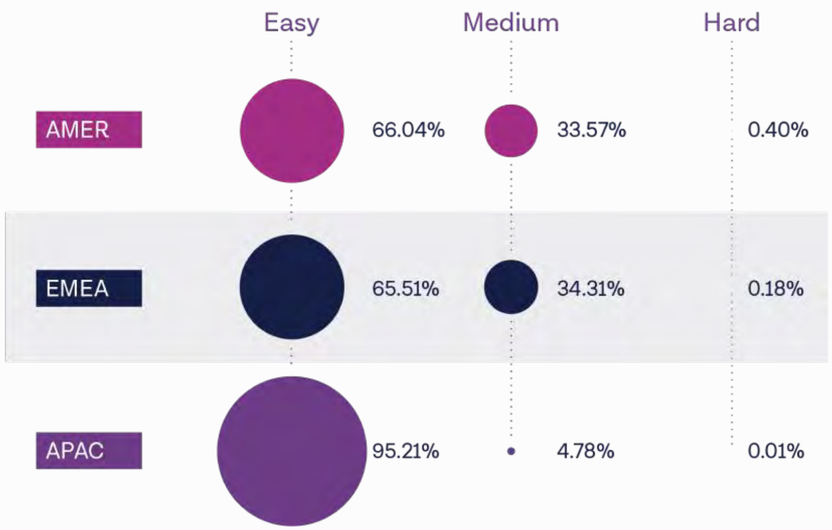
Top fraudulent document
France National ID card

Fraud frontiers: Navigating regional threats

Average fraud rates, by region



Average fraud rates, by region



It's almost impossible to know for sure where fraud originates from geographically. This is because in nearly all cases of fraud, fraudsters hide where they are with VPNs. They consistently change IP addresses to mask their actual location.

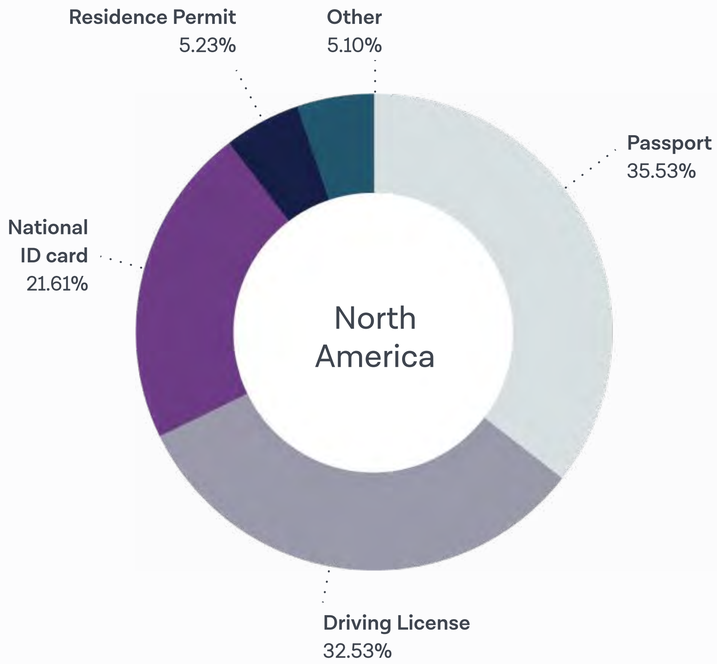
In order to offer the most practical advice, this data examines the fraud trends based on where businesses are based in the world, to determine what threats businesses will see depending on where they operate.

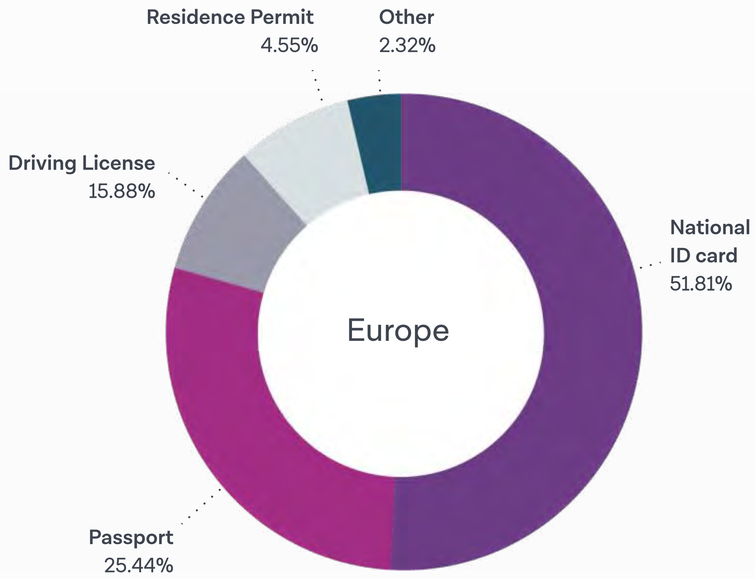
Businesses operating in Asia are more likely to see higher document fraud rates, and slightly higher biometric fraud rates, than in Europe and North America.

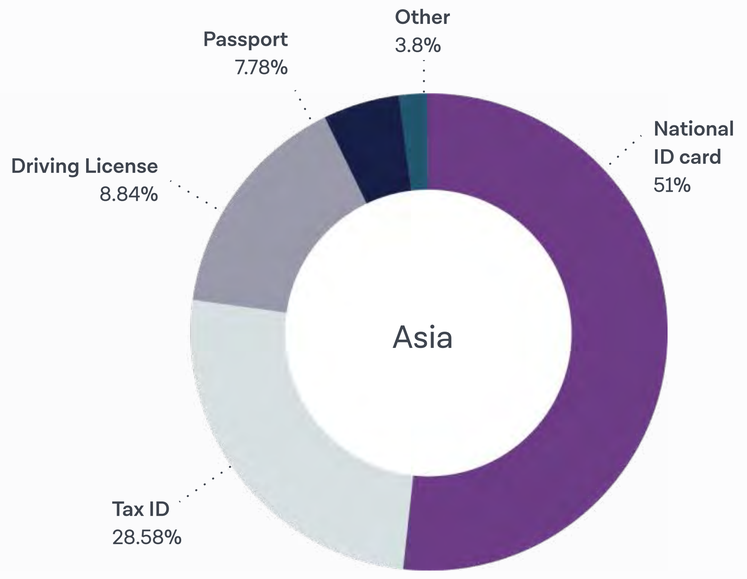
However, Europe and North America see far higher rates of 'medium' fraud. Businesses operating in these regions are therefore more likely to experience emerging sophisticated attack vectors, such as deepfakes, and will need to employ appropriate levels of defense.

Regional realities: Most targeted documents

Fraud by document type







Different regions see different volumes of attacks across different document types. For example, businesses based in North America see more fraud across passports and driving licenses. There's a thriving market in the US for fake driving licenses, hence why this document type sees a high proportion of fraud, alongside passports.

Comparatively, businesses based in Europe and Asia are more likely to see fraudulent National ID cards, which are a far more utilized form of ID in these regions than in North America. It's also worth noting that while European businesses might see a higher proportion of fraudulent passports, businesses based in Asia are more likely to see fraudulent Tax IDs.

Key

- Passport
- Residence Permit
- Driving License
- Tax ID
- National ID Card
- Other

Regional realities: Most targeted documents

Canada Ontario
Driving License

US Florida
Driving Licence
7.4%

UK
Driving Licence
6.8%

US California
Driving Licence
6.4%

US New York
Driving Licence
4.3%

North America

France
National ID card
9.5%

Romania
National ID card
8.4%

France
Passport
8.2%

Italy
National ID card
7.8%

UK
Passport
7.2%

Europe

India
National ID card
16.5%

Philippines
Passport
4.8%

Philippines
Driving License
4.1%

Philippines
National ID card
2.9%

Malaysia
National ID card
1.9%

Asia

05

Interpreting industry insights

Interpreting industry insights

Which sectors see the most fraud?

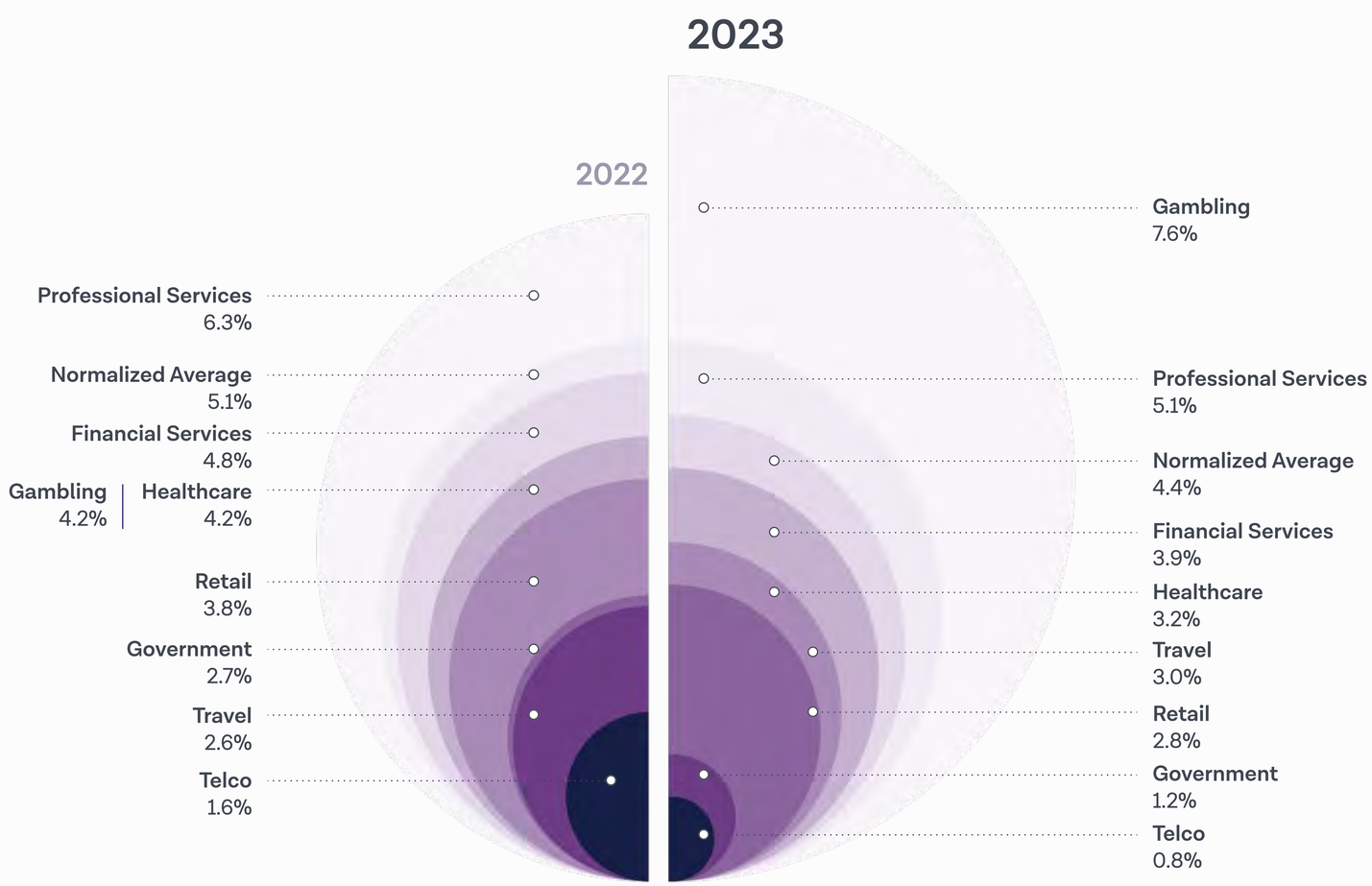
Fraudsters hit the gambling industry hard in 2023. The online gambling space is particularly attractive to fraudsters for two reasons: it's very accessible and there are often cash rewards on the table.

The main types of fraud gambling operators see are:

- **Multiple account creation:** Fraudsters create multiple, even hundreds, of accounts using fake credentials. This gives them better odds, as well as access to more funds, sign-up bonuses and cash rewards.
- **Bonus abuse fraud:** Closely linked to multiple accounts, fraudsters use fake accounts to benefit from sign-up bonuses and other offers.
- **Money laundering:** Criminals sometimes use gambling platforms to hide the original, illegal source of funds.

Professional and financial services also experienced fairly high levels of fraud in 2023. These industries are well aware of the risk fraud poses and often have stringent levels of security in place. They also have high growth targets, so secure customer conversion at onboarding is incredibly important. Given the reward on offer for fraudsters, they remain a target.

Average industry fraud rates



Industry snapshot

Financial Services

Financial services companies generally see two types of fraud. Money laundering and loan theft. Money laundering, where criminals open an account specifically to hide the origin of illicit funds, normally suggests organized crime is involved. Loan theft, where criminals gain access to large amounts of cash and then disappear with the money, can be undertaken by rogue fraudsters, as well as fraud rings.

One way fraudsters undertake both of these attacks is via sleeper accounts. These accounts will look genuine to begin with, before the criminal 'busts out' and takes advantage of the account.

Gambling

The gambling industry sees a lot more digital document fraud than any other industry. The industry tends to offer a lot of sign-up and referral bonuses, which are an attractive honeypot to fraudsters.

However, bonus rewards are generally small, so the scale of attacks must be high to reap the rewards.

Digital attacks are easy to scale, especially when incorporating AI tools, so can help maximize returns. Gambling companies should also take note that fraudsters tend to lean towards using National ID cards and tax IDs.

We believe this is due to the dominance of a handful of specific nationality documents, that are easier to manipulate, after new campaigns in those countries.

Travel

The travel industry sees a higher proportion of physical counterfeits than most other industries.

This is because when collecting a rented vehicle, for example, people are often in a physical location and will need a physical document with them. Unsurprisingly, driving licenses top the list of targeted document types.

Financial Services

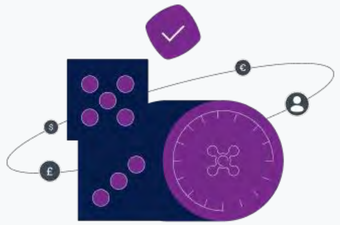
Average fraud rate
3.9%

Fraud sophistication
Easy (78.6%)

Predominant technique
Physical counterfeits (74.8%)

Most targeted document types
National ID cards (47.8%) and Passports (25.9%)

Gambling



Average fraud rate
7.6%

Fraud sophistication
Medium (66.4%)

Predominant technique
Physical counterfeit (44.2%)
closely followed by digital forgeries (41.6%)

Most targeted document types
National ID cards (61.2%) and Tax IDs (28.4%)

Travel

Average fraud rate
3.0%

Fraud sophistication
Easy (92.5%)

Predominant technique
Physical counterfeit (81.9%)

Most targeted document types
Driving Licenses (57.5%) and National ID cards (25.7%)

Preventing fraud

Onfido's recommendations to keep businesses safe

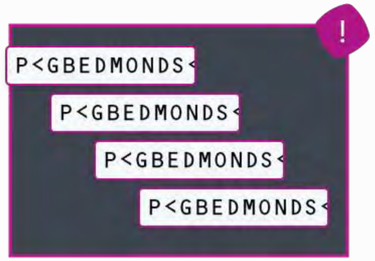
Adopt a layered approach to fraud detection

Fraud manifests differently at each stage of the customer journey, but onboarding is a business's first line of defense. Stopping fraud at the door increases security further down the line.

The Onfido Real Identity Platform allows businesses to orchestrate a range of verifications and signals to build confidence in customers' identities, without unnecessarily increasing the barrier for genuine customers.

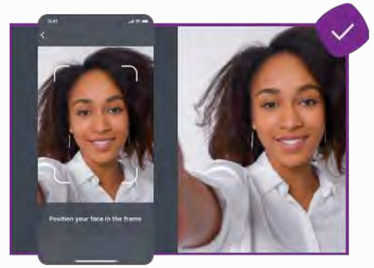
Document Verification

End users take a photo of their identity document and Onfido uses AI to verify the document's authenticity.



Repeat Attempts

Fraudsters tend to re-use information (such as names and document numbers) across multiple fake documents. Repeat Attempts identifies such duplicate information.



Biometric Verification

Onfido offers three forms of Biometric Verification: Selfie, Video and Motion. End users simply capture their face and Onfido compares the photo on the ID to their biometrics.

Known Faces

Identifies repeat fraudsters and signals when a duplicate face has entered a business' system.

Data verification

Validates customer identities against a range of trusted data sources, including global databases; watchlist, sanctions, and PEPs lists; and automated proof of address.

Fraud detection signals

Device intelligence, geolocation, and repeat fraud signals work in the background to detect fraud without impacting UX.

Over the last year, Onfido has helped prevent

$3.9B

in fraud losses for our global client base

Adopt active biometric verification

Motion is Onfido's answer to emerging biometric fraud vectors, such as deepfakes. Powered by fraud-detecting AI, Motion is a 100% automated solution that simply requires users to turn their heads. It's built to offer customers a seamless UX, while delivering highly accurate anti-spoofing capabilities that protect against sophisticated attacks such as deepfakes and injection attacks. It's proven to deliver a 10X anti-spoofing performance improvement with 95% of checks returned in less than 15 seconds.

Leverage AI to mitigate emerging fraud

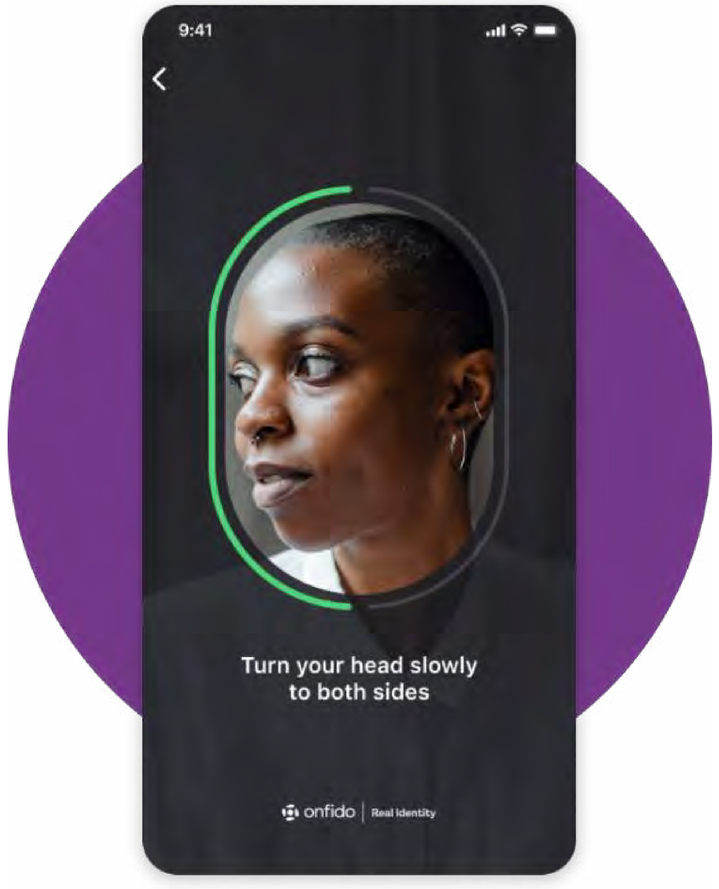
Fraudsters are increasingly turning to digital manipulation and AI-assisted tools in their pursuit of fraud. To counter such attacks, businesses and identity verification providers should leverage AI in their own defense.

Onfido's Atlas™ AI uses unique micro-model architecture combining over 10,000 machine learning models trained to detect specific fraud markers. Atlas detects up to 50% more document fraud than approaches using generalized models.

Use SDKs over APIs

At Onfido we provide a set of SDKs for our customers to integrate an optimized, accessible document and face capture flow into their own apps. Alternatively, the Onfido API enables clients to submit verification checks programmatically.

We would recommend using SDKs over APIs, for the following reasons. Using the SDKs means easier and more flexible integration, more consistent image quality, accessible UX, and better fraud deterrence. We see fewer suspected fraudulent cases via our SDKs because live capture greatly reduces the chance of digitally tampered image submission, while our device integrity checks ensure the authenticity of captures.



Prepare for the fraud of tomorrow

Onfido is dedicated to understanding what and how the next sophisticated threat vectors will attempt to compromise your business. To do this, we built our own Fraud Lab, dedicated to researching the fraud risks of tomorrow.

The Onfido Fraud Lab helps us do three things:

1. **Create quality fraud samples:** We create our own fraud, in-house. Not only to better understand emerging fraud vectors but to train our own Atlas™ AI against them.

2. **Identify emerging attack patterns:** We can replicate emerging attack patterns as soon as we encounter something new to close vulnerabilities, fast.

3. **Build better products:** Our experts think like fraudsters to help predict future attack vectors, so we can develop our products to defend against them.