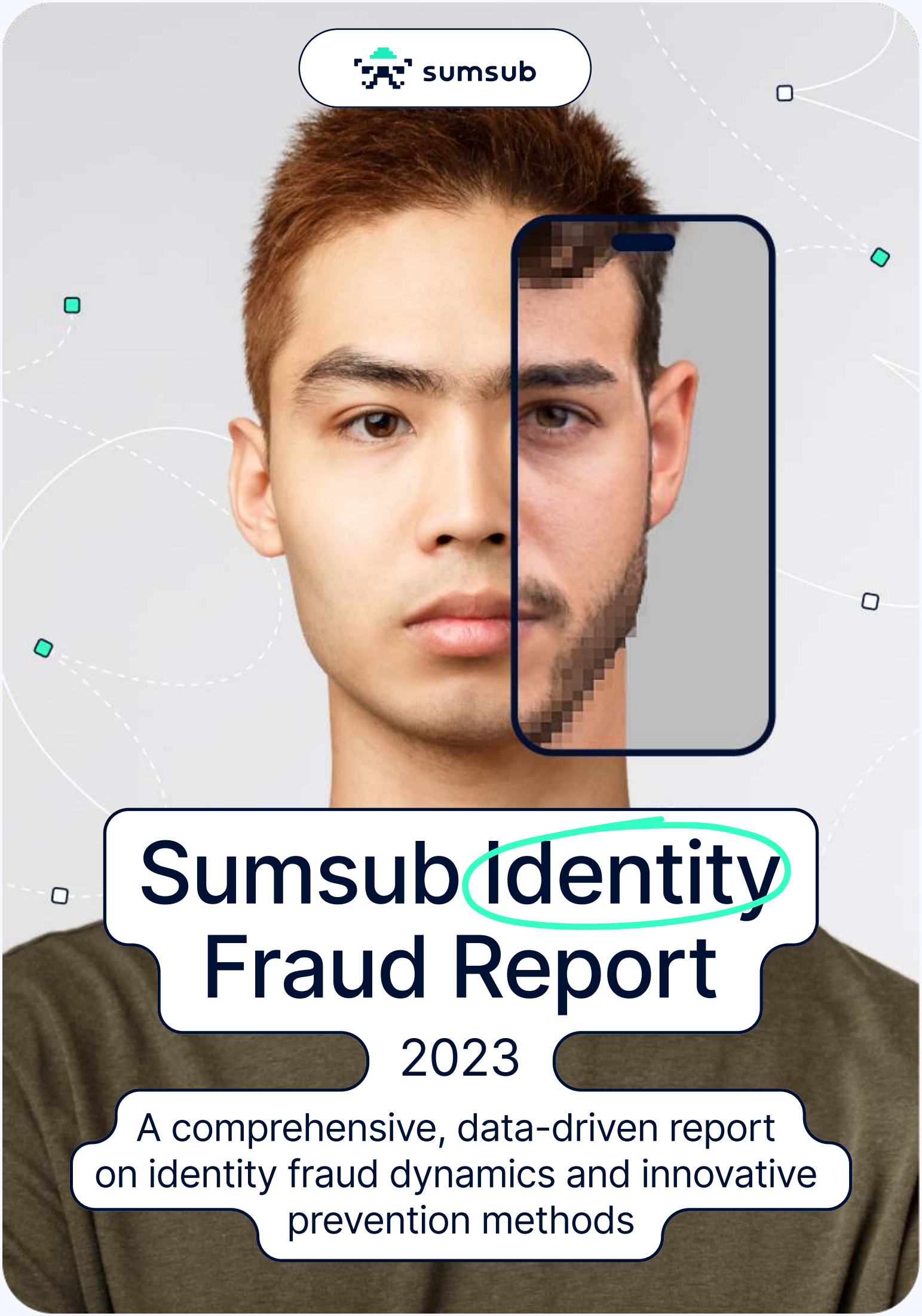
sumsub



Sumsub Identity Fraud Report

2023

A comprehensive, data-driven report on identity fraud dynamics and innovative prevention methods

1. About this report 03

2. Key findings 04

3. Current identity fraud landscape 08

Main identity fraud trends in 2023

Fraud on the move: Rates and dynamics

Identity fraud across regions

Most vulnerable industries revealed

Document types: Genuine or forged?

6. Artificial intelligence: Friend or foe? 33

7. Identity fraud forecast for 2024 42

8. How to fight identity fraud 45

About this report

This report provides a comprehensive analysis of identity fraud across industries and regions. The term "identity fraud" refers to the unauthorized use of personal data or fake identity for malicious activity.

This study compares data from 2022 and 2023. In certain cases, 2021 data is also taken into account to observe trends.

The sections that follow analyze trends, patterns, and changes in identity fraud to gain valuable insights. The study combines internal data with input from internal and external experts, providing well-rounded conclusions on the state of identity fraud in 2023.

The three main sources of data used in this report

2,000,000+	fraud attempts
224	countries and territories
28	industries

All graphs and infographics are based on internal statistics compiled from the data of consenting customers. The data has been aggregated and anonymized.

Key findings

1. AI: A double-edged sword:

Takeaway 1: Artificial intelligence is being used for both malign and legitimate activity at increasing rates.

Insight: The rise of artificial intelligence is reshaping how fraud is perpetrated and prevented. AI serves as a powerful tool both for anti-fraud solution providers and those committing identity fraud. Organizations and individuals must navigate this complex terrain with caution, staying vigilant in the face of AI-driven threats.

2. Collaborative defense against fraud:

Takeaway 2: Anti-fraud companies must make their technologies more accessible by exchanging knowledge and experience.

Insight: The fight against fraud is a collective effort. Companies in the security technology sector must prioritize collaboration, knowledge sharing, and open technology development. This approach empowers the entire industry to stay ahead of increasingly sophisticated fraud tactics.

3. Credibility vs. falsifiability:

Takeaway 3: Documents from developed economies are increasingly forged by fraudsters.

Insight: Since documents from developed economies are often seen as more credible, they're becoming new targets for fraudsters. Therefore, it's imperative for organizations and individuals to recognize the need for enhanced document verification, even from seemingly trustworthy sources.

4. The surge of targeting non-regulated entities:

Takeaway 4: Non-regulated entities are getting targeted more often.

Insight: In an era where regulatory frameworks play a crucial role in shaping security practices, non-regulated entities find themselves increasingly susceptible to the evolving tactics of fraudsters. The absence of stringent regulations places these companies in the crosshairs, demanding a proactive and adaptive approach to fraud prevention.

Top 5 identity fraud types in 2023

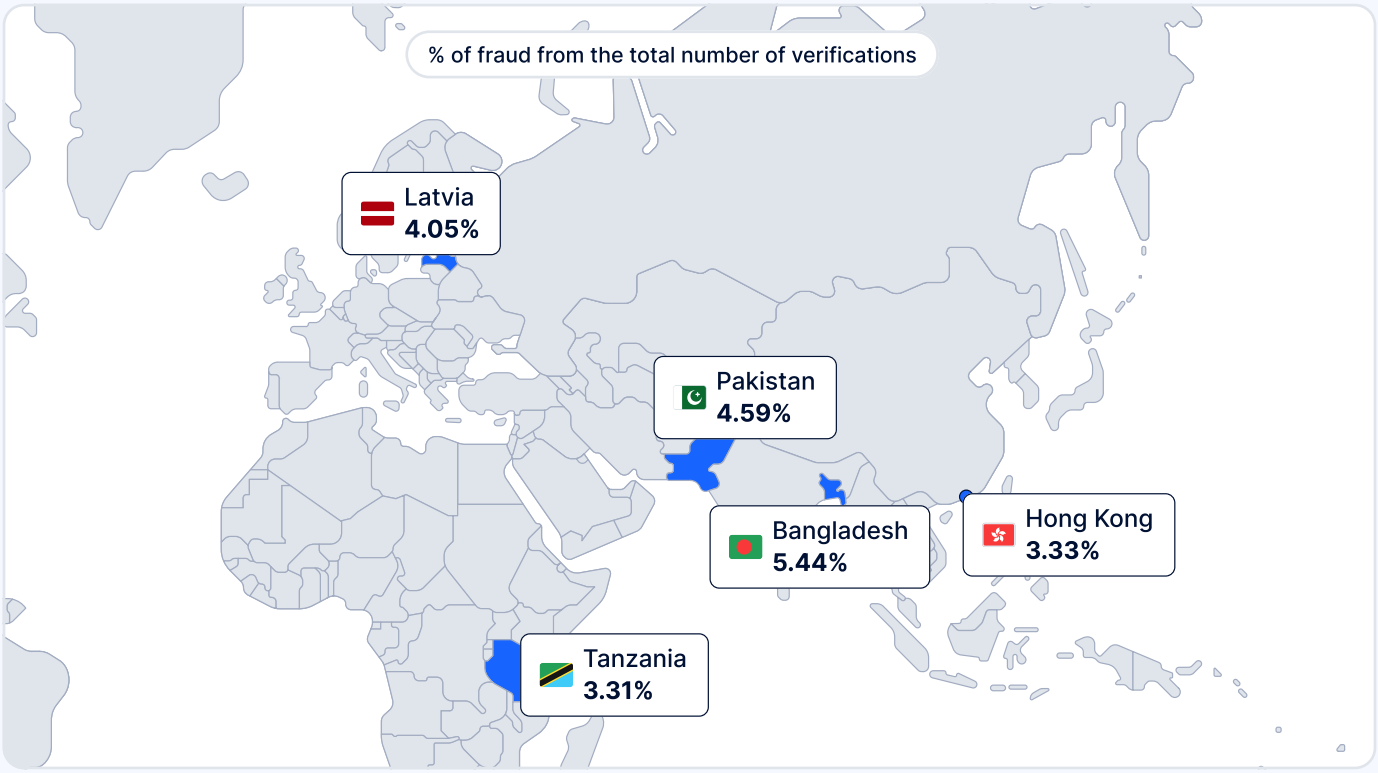
- AI-powered fraud (mainly deepfakes)
- Money muling networks
- Fake IDs
- Account takeovers
- Forced verification

Most trending type of fraud in 2023

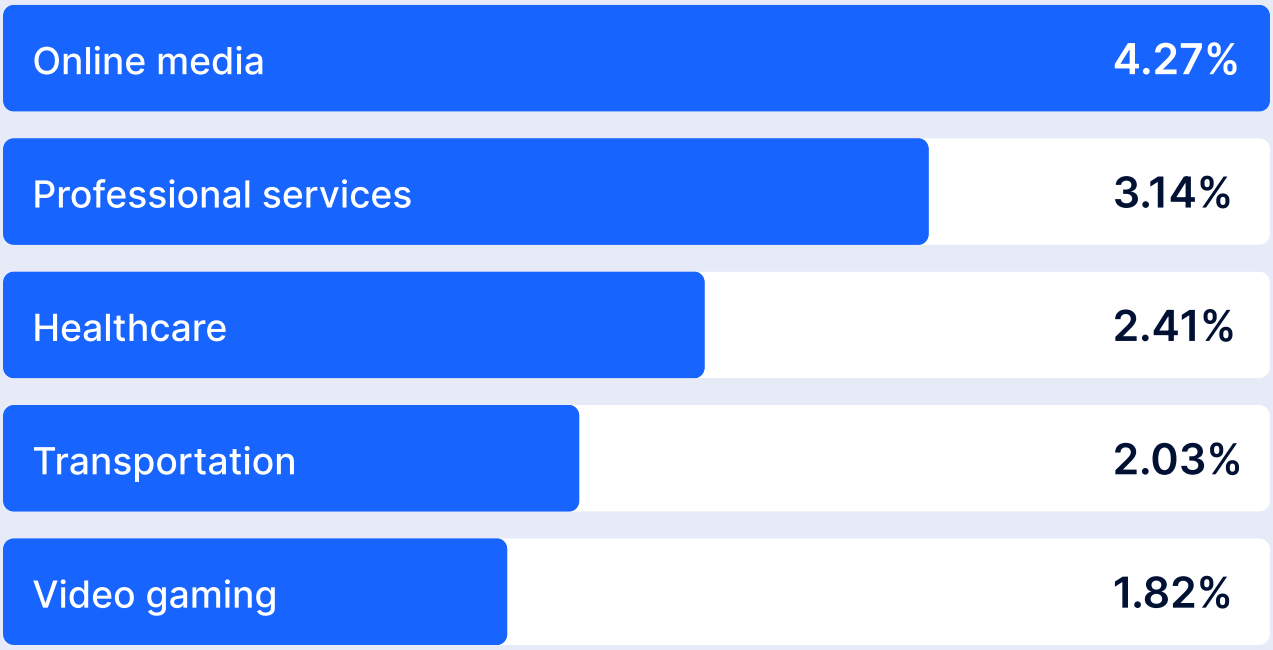
×10 increase in the number of deepfakes detected worldwide from 2022 to 2023 (our internal statistics)

Countries most vulnerable to identity fraud

(fraud cases per total number of applicants by country)



Top 5 industries with the highest percentage of fraud



Most vulnerable document type	ID card
Most forged document	UAE passport
Most popular scheme	Money muling
The country attacked by deepfakes the most	Spain
Region where fraud increased in every country	LATAM
Industry with the highest identity fraud increase	Online media

Current Identity fraud landscape

Main identity fraud trends in 2023

In Sumsub's Identity Fraud Report 2022, the top 3 fraud trends identified were deepfake usage, complex fraud patterns, and advanced forgeries. In 2023, these trends not only persist, but also continue to evolve dynamically.

Deepfake usage

In 2023, deepfake technology continues to pose a significant threat in the realm of identity fraud. The widespread accessibility of this technology has made it easier and cheaper for criminals to create highly realistic audio, photo, and video manipulations, deceiving individuals and fraud prevention systems.

Our internal statistics show a 10x increase in the number of deepfakes detected worldwide from 2022 to 2023.

Pavel Goldman-Kalaydin

Head of AI/ML at Sumsub

Depending on their skills, fraudsters can try to deceive the system in a variety of ways—from simply wearing a mask to creating complex deepfakes, which use machine learning to either generate a fake persona or impersonate an existing person using manipulated photos and videos of them.

Audio deepfakes are actively being used to scam people to penetrate accounts. For example, a Vice journalist successfully entered his own bank account using an AI replica of his voice.

In addition, the proliferation of deepfake technologies is leading to cases of media manipulation, leading to several scandals. This included fabricated images depicting an explosion at the Pentagon or the Pope wearing Balenciaga.

Complex fraud patterns

In 2023, identity fraud patterns continued to shift towards more complex and sophisticated techniques, fueling more advanced scams and money laundering techniques.

Among the most common complex fraud schemes is money muling, where seemingly innocent individuals, known as money mules, are recruited to transfer illegally obtained funds, disguising their origin.

Client case

Crypto money muling scheme

One of the most significant cases was a big layering scheme that affected users from France (mostly), Italy, Portugal, and Spain. Fraudsters tried to transfer fraudulent funds by performing multiple bank transfers to mules to then exchange to crypto and send to well-known crypto exchange services to conceal the funds.

The source: customer's answer in the internal survey

Advanced forgery: Fake IDs

With advancements in technology, fraudsters have access to sophisticated tools and techniques to create counterfeit documents that closely resemble genuine ones.

Although some forgeries still use basic techniques like printed images, there is a noticeable rise in the prevalence of document deepfakes and entirely fabricated IDs.

In May 2023, a man in Washington state was sentenced for aggravated identity theft. The fraudulently-obtained data included names, social security numbers (SSN), dates of birth, and account numbers. Stolen identities were used to create false documents, open credit accounts, obtain loans, and make purchases. Authorities found a mobile identity theft lab, containing equipment for producing counterfeit IDs and debit/credit cards.

Andrew Novoselsky
Chief Product Officer, Sumsub

Fraud has evolved as onboarding goes remote. In financial services, travel, and transportation, there is no contact with a live person anymore, which has attracted fraudsters. It also has become easier to create new identities. Now one person can have 100 or 1000 different identities online.

Top 5 identity fraud types in 2023

- AI-powered fraud (mainly deepfakes)
- Money muling networks
- Fake IDs
- Account takeovers
- Forced verification

Two additional identity fraud trends have emerged in 2023: 1) account takeovers (+155% YoY) and 2) forced verification (+305% YoY).

Account takeovers

Despite efforts to bolster security measures, account takeovers have steadily grown. **According to our internal statistics, global account takeover incidents increased by 155% in 2023.**

The enduring threat of account takeovers can be attributed to several key factors:

- **Sophisticated techniques.** Technological advancements enable more sophisticated techniques for malicious actors to compromise user credentials, including phishing attacks and advanced malware.

- **Exploiting human vulnerabilities through social engineering.** Fraudsters manipulate trust and use psychological tactics to deceive individuals into unknowingly surrendering their account information. This human element makes it challenging to detect and prevent such fraud.

- **Exploiting weaknesses in the digital ecosystem.** Fraudsters have become increasingly adept at targeting and exploiting weak links within digital ecosystems. By taking advantage of vulnerabilities in one platform, they are able to gain unauthorized access to others.

To prevent account takeovers, companies need to deploy advanced anti-fraud systems. These systems encompass continuous monitoring of user behaviour and real-time alerts, along with measures like biometric authentication, device intelligence, and more.

Emerging trend: Forced verification

Forced verification is when individuals are manipulated into going through verification for the benefit of fraudsters.

While forced verification isn’t currently widespread, experts are becoming increasingly concerned about its potential impact. **According to our internal statistics, forced verification grew from 0.31% to 3.52% of all fraud globally in 2023.**

> One of the key indicators of forced verification is the presence of suspicious noises during a verification call, such as background conversations or repetitive sounds. Additionally, unusual behavior, such as the use of a phone or other external devices during verification, can also raise red flags.

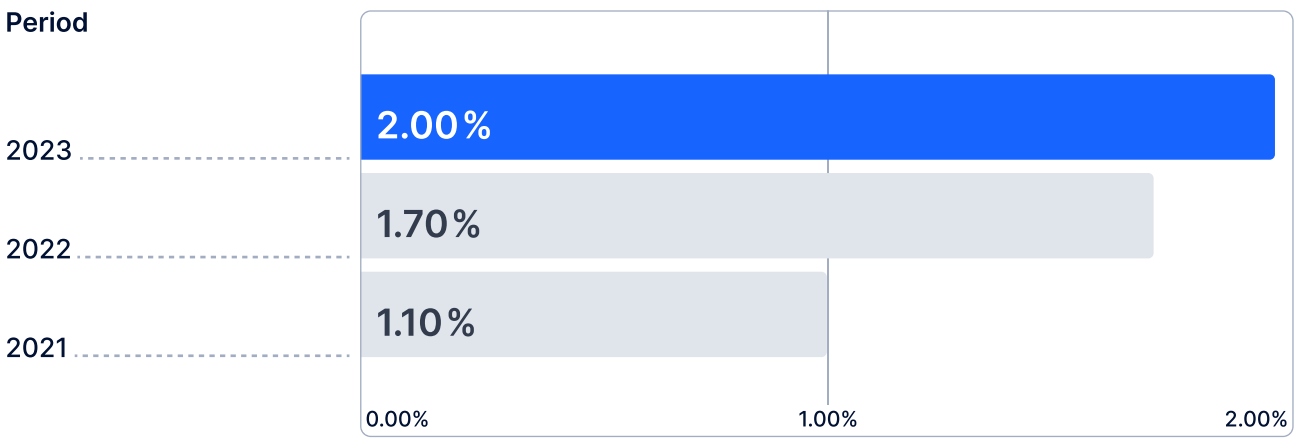
To stop forced verification, it's necessary to deploy AI-based fraud detection systems with voice recognition technologies that can identify and flag anomalies. It’s also necessary to train employees on the signs of forced verification and provide them with guidelines on handling such situations.

Fraud on the move: Rates and dynamics

In the past three years, the fraud landscape has evolved with the development of new technologies, signaling a growing concern for businesses and individuals alike. Based on our findings, there's a discernible upward trend in identity fraud percentages.

The rate of identity fraud has shown a significant increase, nearly doubling from 1.1% in 2021 to 2% in 2023.

Identity fraud rates



% of fraud in all analyzed verification by country

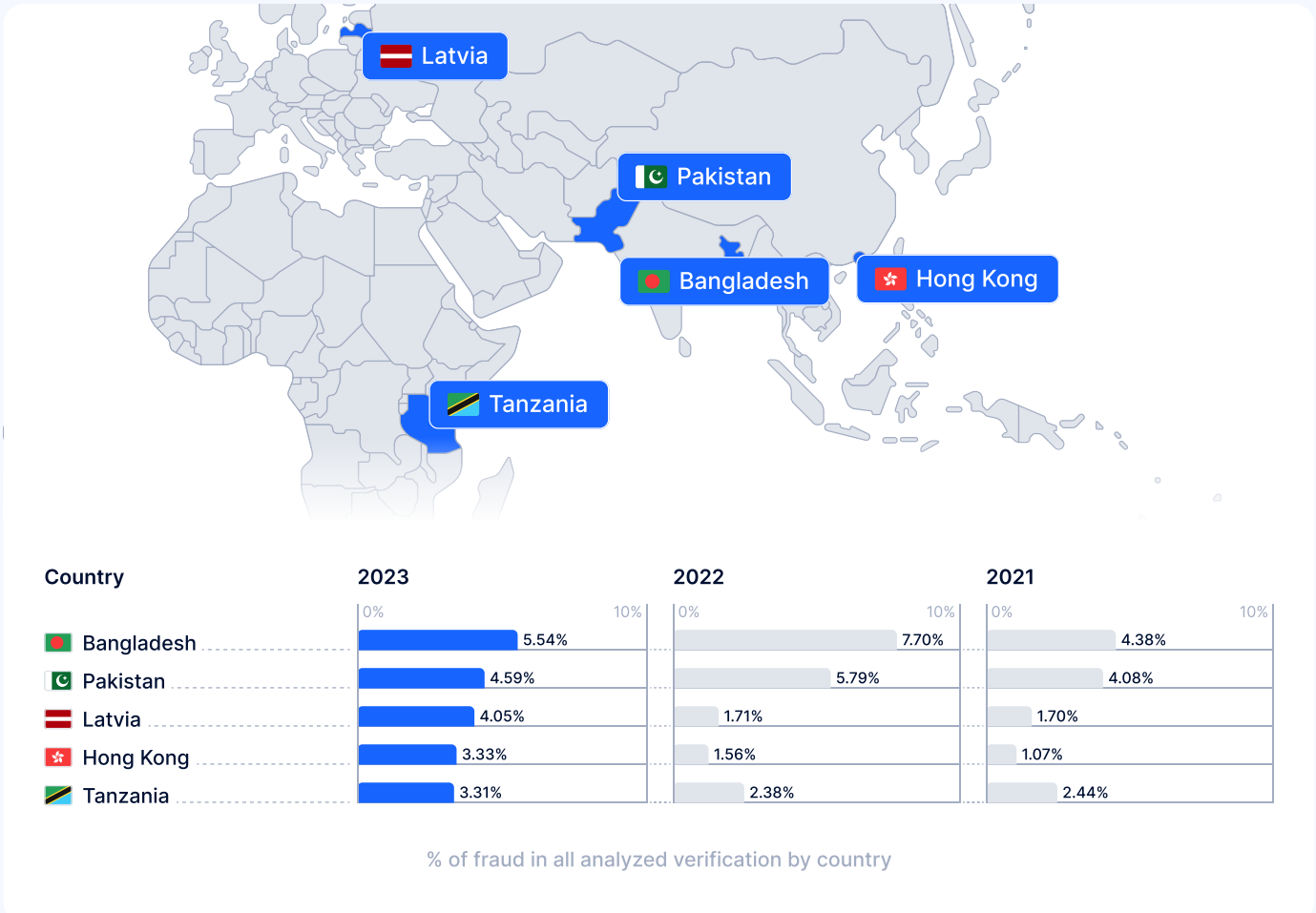
Identity fraud across regions

In 2023, Bangladesh, Pakistan, Latvia, Hong Kong, and Tanzania witnessed the highest rates of identity fraud.

Bangladesh and Pakistan were the most vulnerable countries to fraud in 2021 and 2022. They continue to top the list in 2023, although rates have decreased over the year.

Remarkably, identity fraud rates in Latvia and Hong Kong have more than doubled this year compared to 2022, joining the top 5 countries prone to fraud.

Top 5 countries with the highest identity fraud rates



Andrew Novoselsky
Chief Product Officer, Sumsub

We're seeing an even increase in attempted foul play around the world. In the Americas and Europe, there are more fraud attempts using AI. In Asia and Africa,the accounts of real people are continuing to be sold for small amounts of money.

Europe

In the past three years, identity fraud rates in Europe have exhibited diverse patterns.

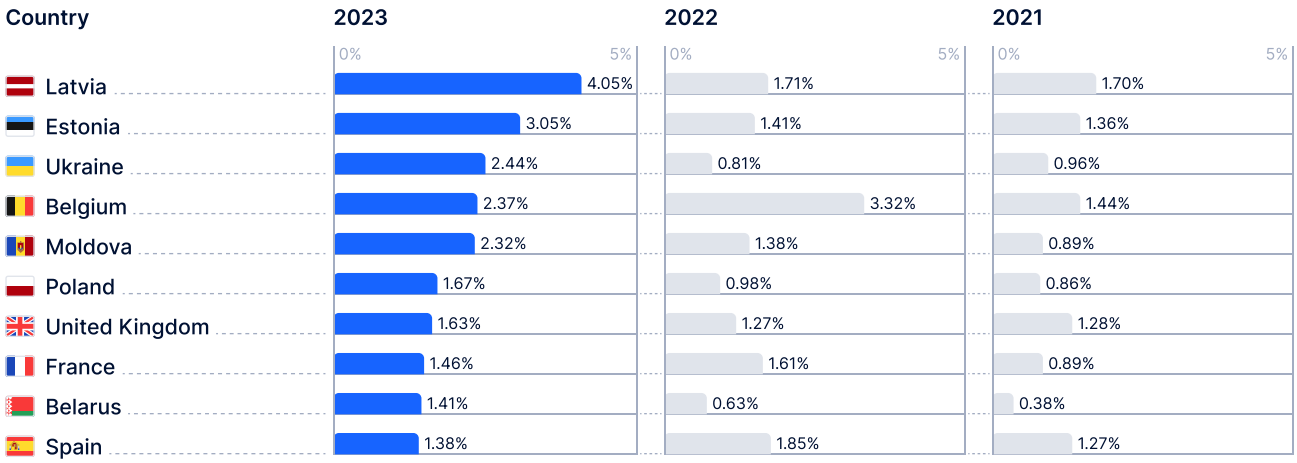
From 2021 to 2023, Latvia, Estonia, and Ukraine have seen a noteworthy increase in identity fraud rates. Latvia experienced a significant jump from 1.70% to 4.05%.

The rise in fraud rates in Latvia can be attributed to the stricter regulations imposed on crypto firms in neighboring Estonia, causing crypto companies to relocate to Latvia. Meanwhile, the fraud reduction impact of Estonia's newly implemented regulations may not have become apparent yet, as they were implemented mid-year.

Other countries like Belgium showed an initial rise in 2022 but slightly dipped in 2023. Hungary, meanwhile, experienced peak rates in 2022 which then decreased the following year.

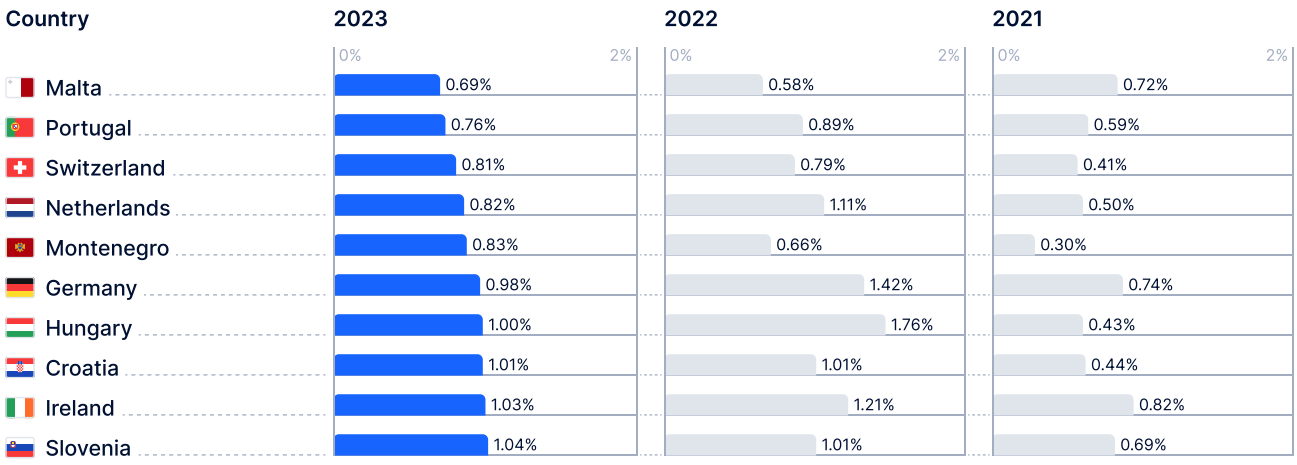
On the other end of the spectrum, countries like Malta, Portugal, and Switzerland have maintained relatively lower fraud percentages throughout the past three years, all staying below the 1% mark in 2023.

Top 10 countries in Europe with the highest percentage of fraud in 2023



% of fraud in all analyzed verification by country

Top 10 countries in Europe with the lowest percentage of fraud in 2023



% of fraud in all analyzed verification by country
The full list of European countries is in the appendix (Chart 1)

Deepfakes

Deepfake attacks in Europe have posed significant challenges to Spain, the UK, and Germany, with each country accounting for over 10% of the total cases in the region. Average growth throughout the region is +780%.

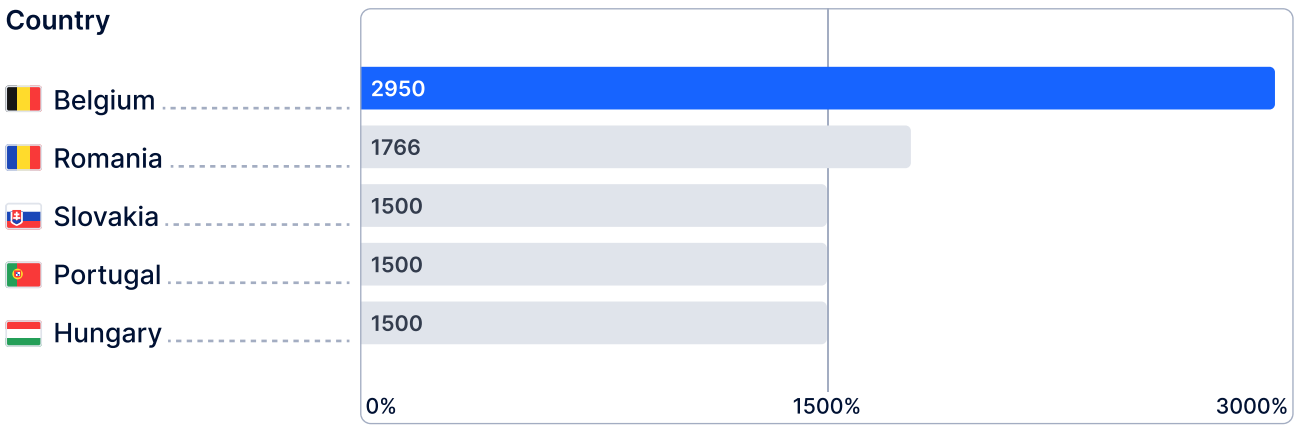
The prevalence of deepfake attacks can be attributed to the attractiveness of these economically-developed countries for fraudsters, as well as their advanced digital infrastructure and significant online presence.

Deepfake fraud in Europe, 2023

Country	
Spain	17.6%
United Kingdom	13.3%
Germany	12.1%
Italy	6.8%
Poland	5.9%
Other *	44.3%

* Ukraine, Sweden, France, Netherlands, Estonia, Czech Republic, Belgium, Switzerland, Romania, Greece, Austria, Belarus, Norway, Lithuania, Finland, Croatia, Slovakia, Hungary, Portugal, Ireland, Denmark, Bulgaria, Malta, Moldova, Serbia, Montenegro

Top 5 European countries by deepfake growth (2022–2023)



The full list of European countries is in the appendix (Chart 2)

Asia-Pacific (APAC)

There was a significant surge in identity fraud rates in Bangladesh and Pakistan in 2022, which notably decreased in 2023.

In 2023, Bangladesh and Pakistan have had the highest fraud rates in both the region and the world, with rates of 5.44% and 4.59% respectively.

Notably, Vietnam experienced an anomalous spike in 2022, reaching 9.94%, before significantly decreasing to 1.38% in 2023.

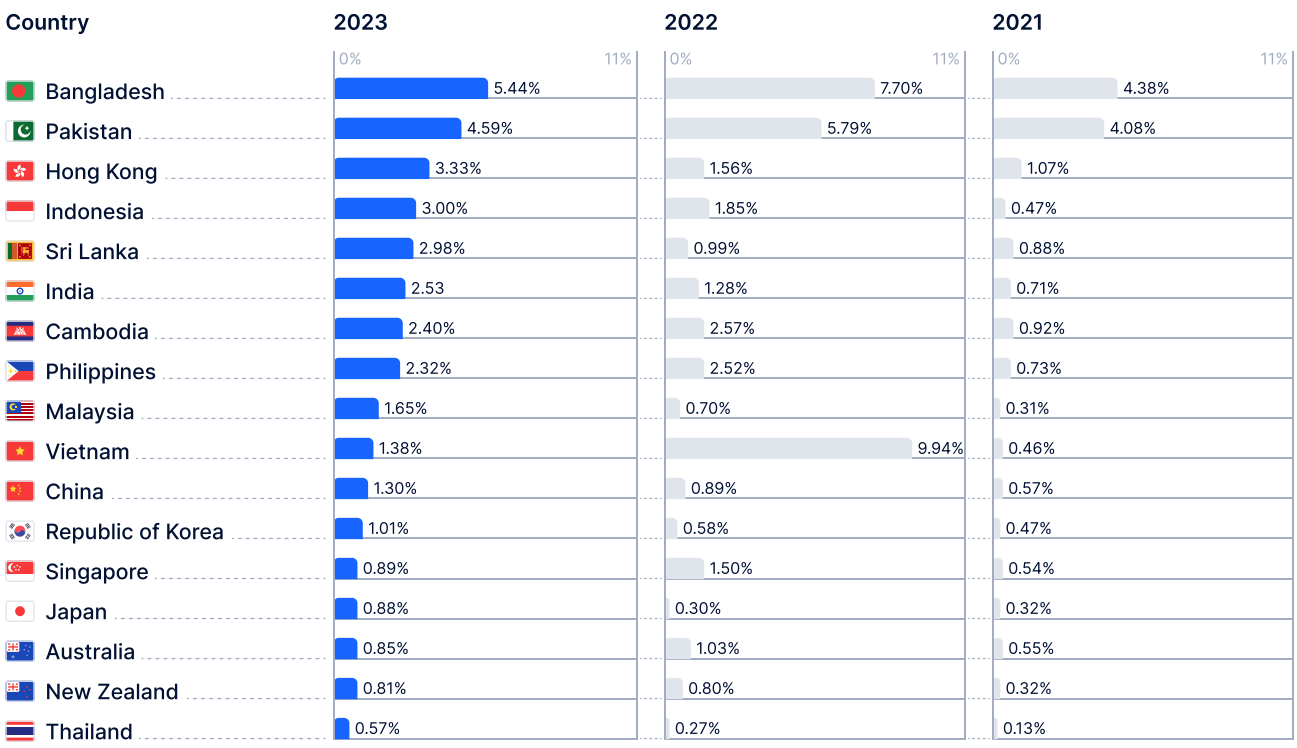
Indonesia, Hong Kong, and Cambodia have more than doubled their identity fraud percentages between 2021 and 2023, indicating a growing concern.

Countries are taking proactive anti-fraud measures. For example, Hong Kong's Monetary Authority published a circular with enhanced measures to protect e-banking from fraudsters in October 2023, including enhanced monitoring for suspicious transactions and additional customer authentication.

Singapore stands out for successfully reducing its fraud rate in 2023, maintaining a low level of 0.89%.

Conversely, nations such as Japan, Australia, and Thailand have remained relatively stable, with percentages staying under the 2% threshold over the years.

Identity fraud rates in APAC, 2021–2023



% of fraud in all analyzed verification by country

Deepfakes

In APAC, deepfakes have increased by 1530%. Vietnam and Japan are leaders in the number of attacks, surpassing other countries significantly.

Japan is known for its use of deepfakes in the entertainment sector, which may enable fraudsters to exploit this technology in other fields.

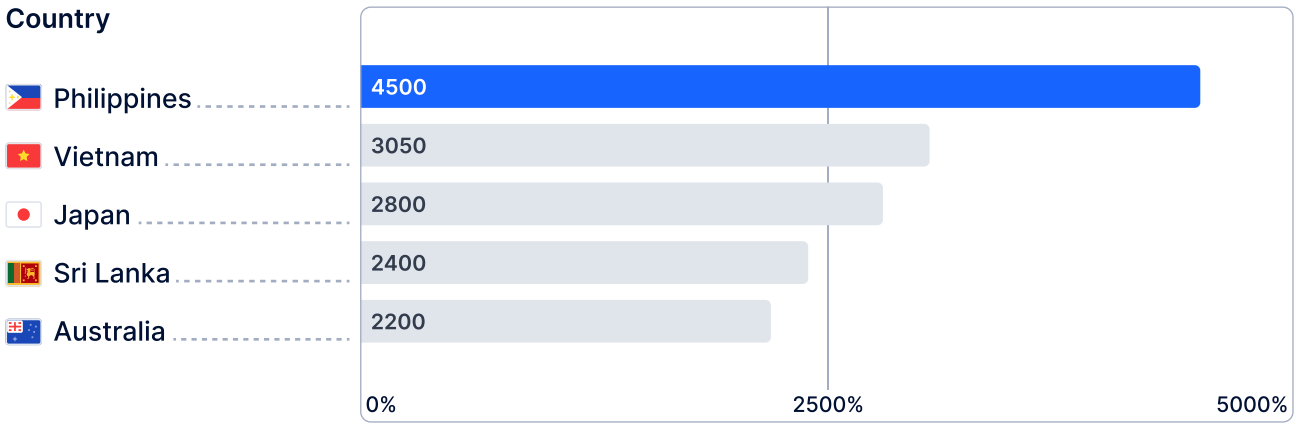
Vietnam, on the other hand, has a growing digital economy and large online population that make it an attractive target for fraudsters.

Deepfakes fraud in APAC, 2023

Country	
Vietnam	25.3%
Japan	23.4%
Australia	9.2%
China	7.7%
Bangladesh	5.1%
Other *	29.3%

* Philippines, Indonesia, Pakistan, Republic of Korea, India, Sri Lanka, Malaysia, Hong Kong, New Zealand, Singapore, Thailand, Cambodia

Top 5 APAC countries by deepfake growth (2022–2023)



The full list of APAC countries is in the appendix (Chart 3)

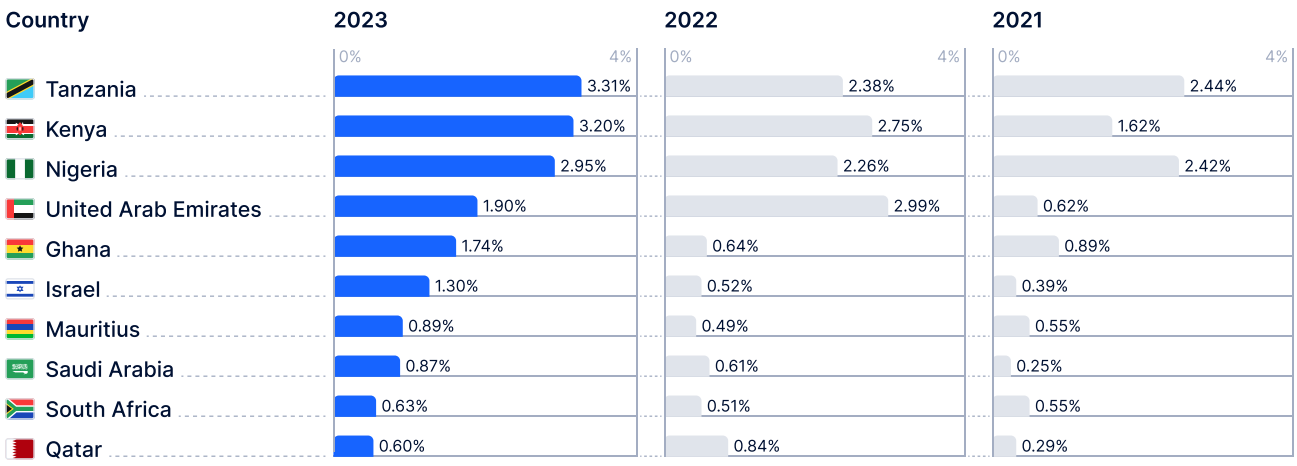
Middle East and Africa (MEA)

In the MEA region, the top 3 countries with the highest identity fraud rates are Tanzania, Kenya and Nigeria.

The largest growth in the region over the past year was shown by Tanzania (+1.1%) and Ghana (+0.93%).UAE and Qatar are two countries in the region that decreased their identity fraud rates in 2023. The UAE saw a substantial increase from a peak of 2.99% in 2022 to 1.9% in 2023.

Meanwhile, countries such as Qatar, South Africa, Saudi Arabia, and Mauritius consistently maintained fraud percentages below 1% for three years.

Identity fraud rates in MEA, 2021–2023



% of fraud in all analyzed verification by country
The full list of MEA countries is in the appendix (Chart 6)

Deepfakes

The MEA region has seen an increase in deepfakes of 450%. The absolute leader is the UAE, which can be linked to its strong online presence, technological advancements, and rapid growth associated with a favorable business environment.

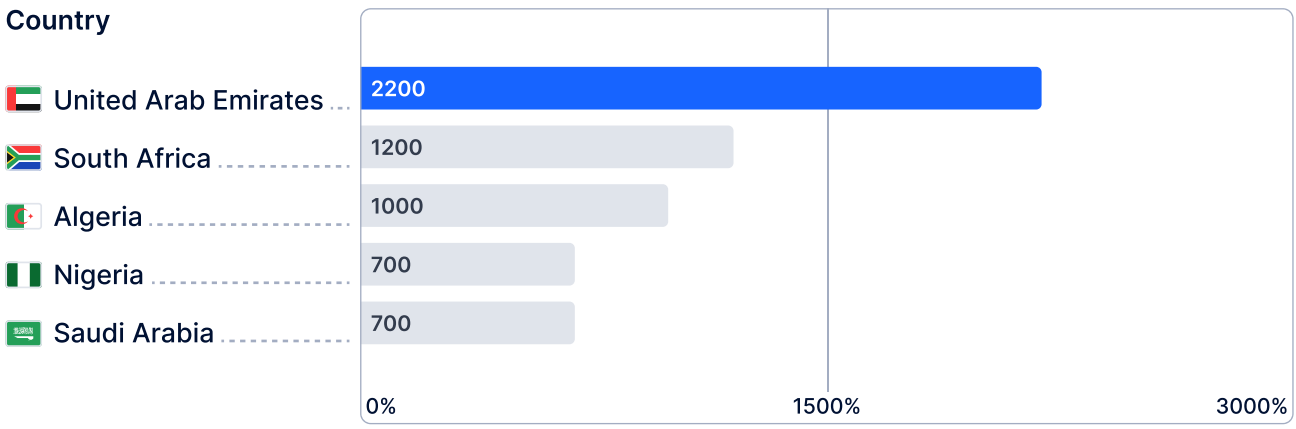
Among African countries, South Africa (19.7%) and Nigeria (11.5%) have faced the highest number of deepfake attacks.

Deepfakes fraud in MEA, 2023

Country	
United Arab Emirates	36.1%
South Africa	19.7%
Saudi Arabia	11.5%
Nigeria	11.5%
Israel	8.2%
Other *	13.0%

* Kenya, Mauritius, Ghana, Qatar, Tanzania

Top 5 MEA countries by deepfake growth (2022–2023)



The full list of MEA countries is in the appendix (Chart 4)

Latin America (LATAM)

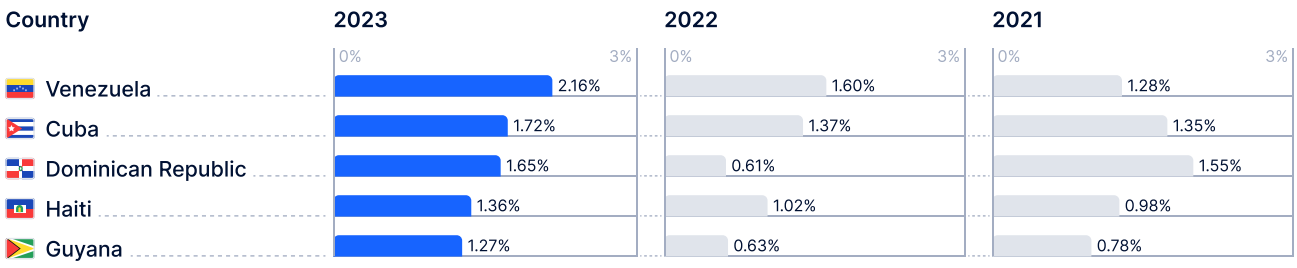
In the LATAM region, identity fraud rates increased in all analyzed countries in 2023.

Mexico saw a substantial increase in identity fraud from 2021 to 2023, nearly tripling from 0.48% to 1.27%. Colombia experienced a similar trend, rising from 0.79% in 2021 to 1.12% in 2023.

While countries like Uruguay and Argentina have seen steady increases over these years, Brazil's identity fraud rate has remained relatively stable.

The rise of identity fraud in Latin America can be attributed to several factors, including the increasing digitalization of transactions, socioeconomic inequalities, informal economies, and more. Compounding the issue, certain fraudsters have demonstrated the ability to forge Portuguese and Spanish-speaking documents, further elevating the risk of identity fraud in LATAM countries.

Identity fraud rates in LATAM, 2021–2023



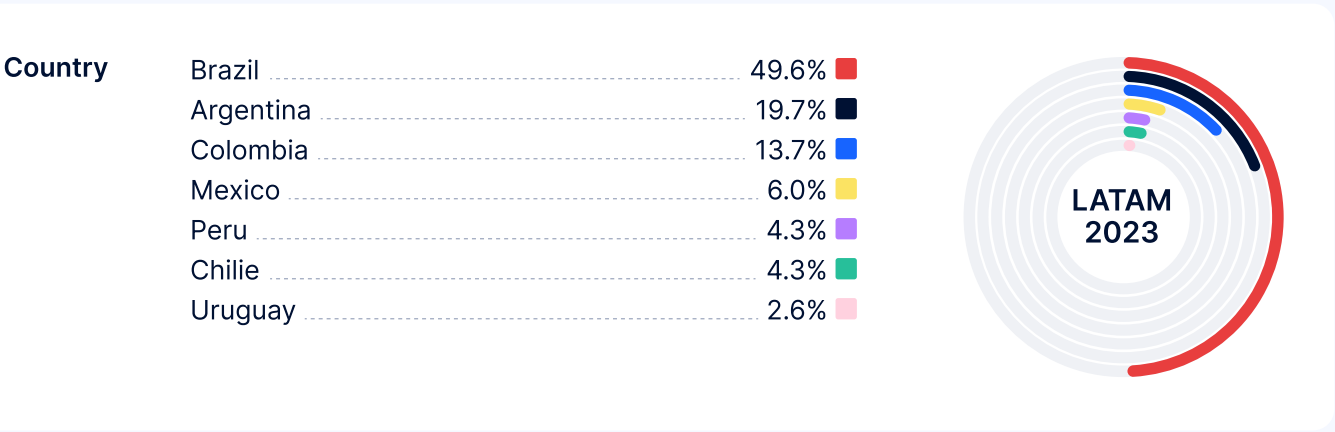
% of fraud in all analyzed verification by country
The full list of LATAM countries is in the appendix (Chart 7)

Deepfakes

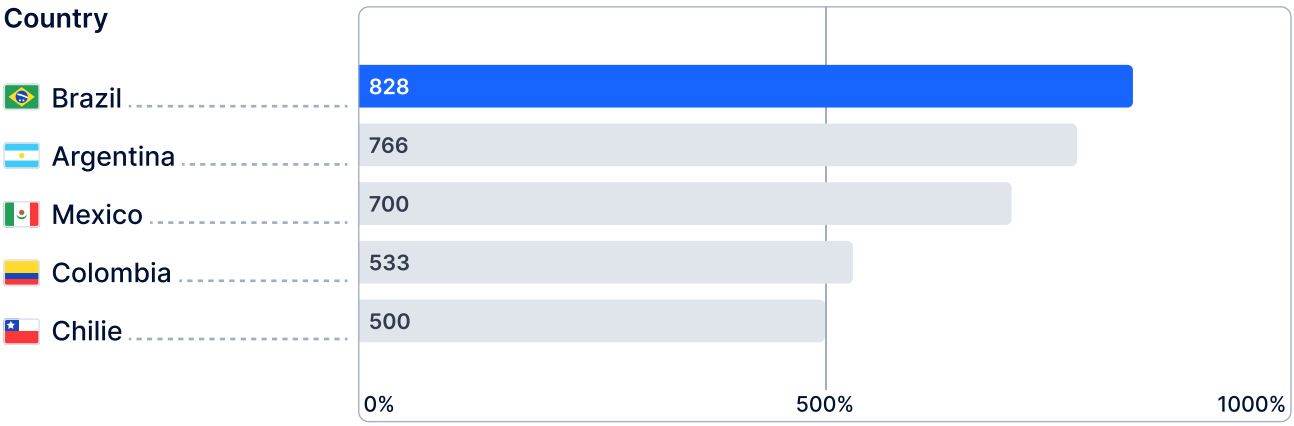
Brazil experiences the highest number of deepfake cases in Latin America, accounting for approximately half of all reported incidents. Most deepfake cases in Brazil are linked to the crypto, fintech and iGaming industries. Average growth throughout the region is +410%.

Argentina and Colombia have also reported a significant number of deepfake cases. Although their shares may not be as large as Brazil's, both countries have a notable amount of deepfake incidents for the region.

Deepfakes fraud in LATAM, 2023



Top 5 LATAM countries by deepfake growth (2022–2023)



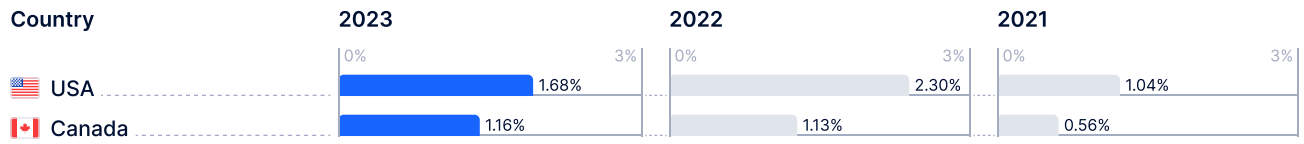
The full list of LATAM countries is in the appendix (Chart 5)

US and Canada

The US and Canada, characterized by their advanced economies and technological landscapes, present an interesting dynamic in the context of identity fraud over the past three years.

The US experienced a significant jump in identity fraud rates from 1.04% in 2021 to 2.30% in 2022, although there was a subsequent decrease in 2023, settling at 1.68%. Canada, on the other hand, demonstrated a more gradual increase, moving from 0.56% in 2021 to 1.16% in 2023.

Identity fraud rates in the US and Canada, 2021–2023



% of fraud in all analyzed verification by country

Deepfakes

The US has emerged as the absolute leader in deepfake fraud incidents.

US advancements in artificial intelligence and digital manipulation technology are leading to a rise in fraud involving fake videos and images. The widespread availability of high-quality media content and the popularity of social media platforms in the US contribute to the propagation of deepfake fraud.

Deepfake fraud in the US and Canada, 2023

Growth of deepfakes in US and Canada (2022–2023)

Average growth throughout the region is +1740%

Most vulnerable industries revealed

The top 5 industries most affected by identity fraud in 2023 are online media, professional services, healthcare, transportation, and video gaming.

Identity fraud tends to target non-regulated industries more often. This is primarily due to a lack of strict regulations and verification requirements, which make it easier for fraudsters to exploit weaknesses.

The online media sector saw the biggest rise in identity fraud (x4), from 1.56% to 4.27% between 2021 and 2023.

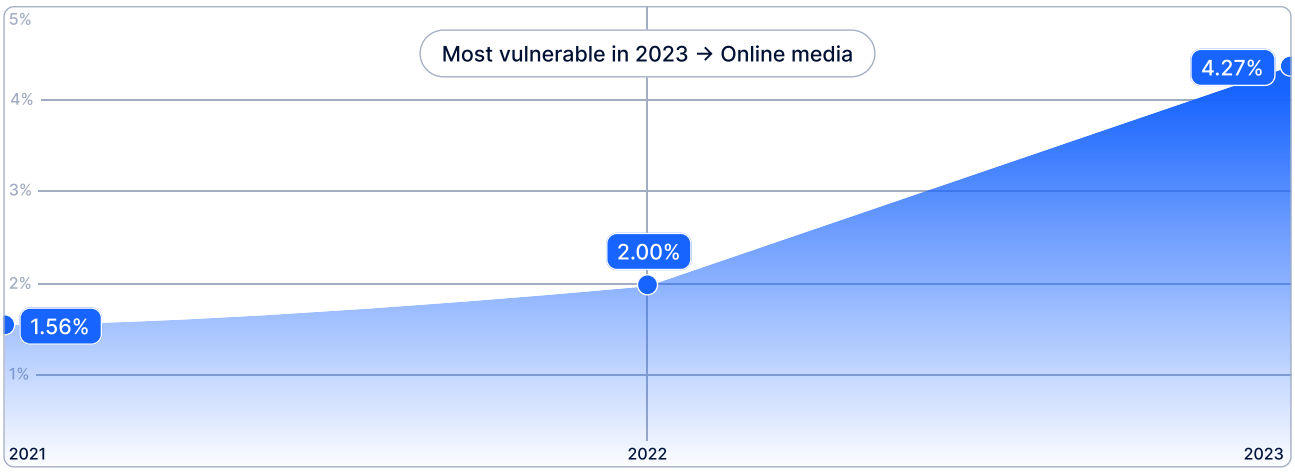
Online media encompassing news websites, streaming services, social platforms, and digital advertising, face an escalating risk of fraud. Large audiences and insufficient regulations create an environment susceptible to fraudulent activities like fake accounts, engagement manipulation, and the spread of misinformation. Experts anticipate companies in this sector to implement stricter rules such as mandatory identification, similar to measures already being taken in China.

Conversely, industries like EdTech remained relatively stable, even showing a slight decrease over the years.

Healthcare saw a considerable leap in 2023, with no reported fraud in 2021 rising to 1.61% by 2023.

Video games had a peak rate of 3.10% in 2022, but saw a dip the following year.

Identity fraud rates by industry, 2021–2023



Category	2023	2022	2021
Online Media	4.27%	2.00%	1.56%
Professional services	3.14%	2.20%	1.18%
Healthcare	2.41%	0.10%	0.11%
Transportation	2.03%	1.00%	0.29%
Video gaming	1.82%	3.10%	1.00%
Crypto	1.77%	1.90%	0.69%
Traditional Finance	1.69%	1.50%	0.45%
Classifieds	1.63%	2.20%	0.41%
Online travel	1.61%	1.30%	0.00%
IT service	1.23%	1.10%	0.93%
Fintech	1.16%	1.40%	0.67%
iGaming	1.04%	0.70%	0.48%
E-commerce	1.02%	0.90%	0.63%
EdTech	0.58%	0.70%	0.64%
Marketplace	0.33%	0.40%	0.07%
Other b2c	0.23%	0.30%	1.22%

% of fraud in all analyzed verification by industry

Deepfakes

The crypto sector stands out as the absolute leader in deepfake cases, followed by fintech. The sector's digitized nature, potential for significant financial gain, and ongoing regulatory challenges create vulnerabilities that fraudsters exploit.

Deepfake fraud by industry, 2023

Industry	
Crypto	87.7%
Fintech	7.7%
iGaming	1.6%
Professional services	1.2%
E-commerce	0.5%
Other *	0.5%

* Video gaming, IT service, Online Media, Classifieds, Traditional Finance, Other B2C, Transportation

Luke Raven

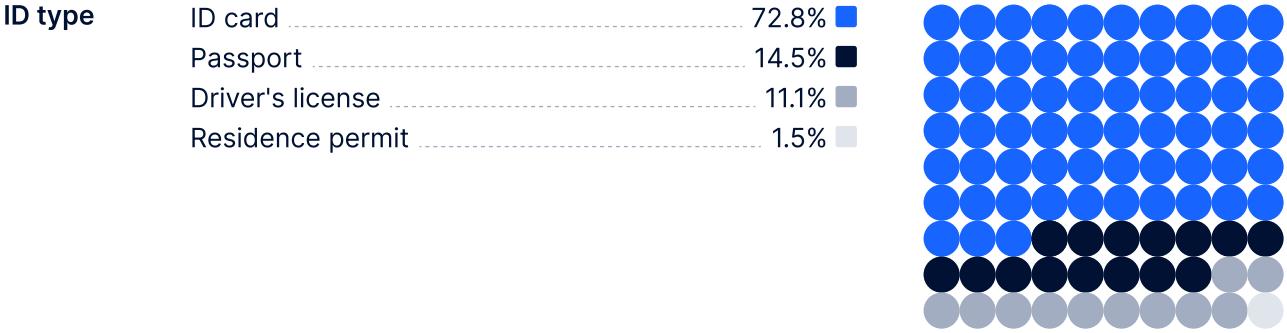
Fraud and Financial Crime Expert

Collaboration across sectors is vital to combat fraud effectively. There is a need to go beyond traditional partnerships like bank-to-bank or crypto-to-crypto. Breaking down silos and sharing information between different participants boosts prevention, detection, and the response to fraud. This can enhance fraud trend identification, illicit transaction tracing, and technology development.

Document types: Genuine or forged?

ID cards remain the most frequently exploited for identity fraud, accounting for nearly 75% of all fraudulent activities involving identity documents.

Fraud percentage by identity document type, 2023

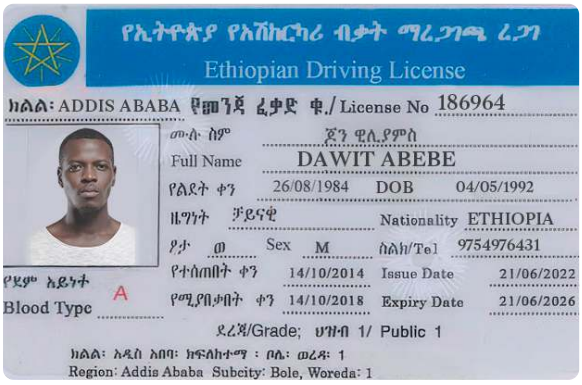


In 2023, fraudsters are increasingly targeting developed countries for forging documents.

The percentage of fake IDs in these countries has risen by an average of 163%, while the percentage of fake passports has increased by an average of 147%.

The UAE passport
is the most forged identity document, with every 4th passport forged

The Brazilian driver's license
is least forged globally



The Ethiopian driver's license
has had the world's fastest growth in forgery cases

A breakdown of the top 10 countries by ID, passport, and driving license forgery can be found in the appendix: Charts 8–10.

Artificial Intelligence: Friend or foe?

Artificial Intelligence (AI) has revolutionized the fight against fraud, but it comes with its own set of challenges. While AI can be a powerful weapon in preventing fraud, it can also be exploited by fraudsters who use it to their advantage.

As we continue to combat identity fraud, it's important to harness the potential of AI while also staying one step ahead of those who seek to exploit it.

AI: A Defender's Shield

AI is a formidable defense against the rising tide of identity fraud. As fraud tactics grow in sophistication, AI-driven fraud prevention solutions have become an indispensable asset for organizations and individuals alike.

Machine learning models can analyze vast datasets, identifying unusual patterns and anomalies that may indicate fraudulent activity. Natural language processing (NLP) algorithms can be employed to detect phishing emails and fraudulent messages, shielding users from social engineering attempts. AI systems can even verify identities with biometrics, reducing the risk of unauthorized access.

AI-driven fraud prevention isn't merely reactive; it's also predictive. Advanced algorithms can anticipate emerging fraud trends and continuously adapt to new attack vectors.

This proactive approach empowers organizations to stay one step ahead of fraudsters.

Case 1

Fraud networks

AI is a powerful tool for detecting fraud networks. Traditional fraud detection mechanisms might vet an applicant at the point of entry (onboarding) and deem them legitimate if they meet the required criteria. However, this method can miss cunning fraudsters who initially appear legitimate only to engage in fraud later on.

But scrutiny shouldn't end after onboarding. Instead, continuous monitoring and analysis ensure that even those applicants who've passed initial verification are consistently under observation. Should they show signs of fraud after being onboarded, they won't go unnoticed. This proactive approach ensures that fraudsters are caught in their tracks, safeguarding both the platform and its users.

Case 2

For Fake's Sake

In today's landscape, the battle against identity fraud requires a united front, highlighting the need for collaboration. By sharing knowledge, resources, and technologies, companies can collectively strengthen their defenses and stay one step ahead of fraudsters.

In October 2023, Sumsub released For Fake's Sake, a set of machine learning-driven models enabling the detection of deepfakes and synthetic fraud. Sumsub has vast experience analyzing visual data and differentiating real individuals from AI-generated fake personas.

The For Fake's Sake tool is made available to all to download for free and use. Following this initial contribution, Sumsub will leverage feedback from the AI-research community to further improve the model's capabilities.

AI: A fraudster's arsenal

Fraudsters are quick to adapt to technological advancements, and AI is no exception. Deepfakes, one of the most notorious offshoots of AI, exemplify how this technology can be weaponized for malicious purposes.

Deepfakes employ AI algorithms to create hyper-realistic videos, audio recordings, or documents, making it challenging to distinguish between genuine and fabricated content. This paves the way for identity theft, scams, and misinformation campaigns on an unprecedented scale.

×10 increase in the number of deepfakes detected worldwide from 2022 to 2023 (our internal statistics)

Pavel Goldman-Kalaydin

Head of AI/ML at Sumsub

So long as AI technologies continue to develop, more sophisticated synthetic fraud will emerge, particularly impacting any industry onboarding customers online without face-to-face communication. We've seen deepfakes become more and more convincing in recent years and this will only continue and branch out into new types of fraud, as seen with voice deepfakes. Both consumers and companies need to remain hyper-vigilant to synthetic fraud and look to multi-layered anti-fraud solutions, not only deepfake detection. This could be behavioral anti-fraud and transaction monitoring to pick up what the human eye may not be able to detect.

As AI-powered fraud increases, countries are starting to take proactive measures to introduce regulations. They are aimed at safeguarding business and individuals against the harmful impacts of AI as a whole, including the negative effects of deepfakes.

Deepfake regulation

Regulation surrounding deepfakes is still in its early stages, just like regulation around AI.

The reason for that is quite simple: Deepfakes are a clear example of a dual-use technology. They can be deployed for well-intended purposes just as well as harmful purposes. So, any attempt to limit it should not only strive to achieve a balance between regulation and tech innovation, but also between limitation and freedom of speech (e.g. deepfakes can also be deployed in evidently creative ways, and limiting the technology in such circumstances could be an infringement upon freedom of speech).

Here is a summary of the primary efforts to regulate deepfakes in four key jurisdictions.

China

China is ahead of any other country when it comes to deepfake regulation. The "Regulations on the Administration of Deep Synthesis of Internet Information Services" was approved by the Chinese Cyberspace Administration Authority (CAC) in December 2022, enacted in January 2023, and came into force in August 2023. Key points of the regulation include:

- Users must consent to their images being used in and by “deepfake” technology.
- Deepfakes cannot be used for the purposes of spreading fake news.
- Deepfake services need to authenticate the identity of users.
- Deepfake content must come accompanied with a warning informing users that the content is AI generated.
- Deepfake content that goes against existing laws is prohibited.

While there are obstacles in enforcing this regulation, which can also be seen as an attempt by the government to crackdown on anti-regime deepfakes, it is important to highlight China’s trend-setter role in the regulation of deepfakes.

EU

The EU has been trying to tackle the issue of deepfakes through different policies and angles. Yet, it still lacks a single approach aimed exclusively at regulating deepfakes, as China has. The EU's proactive and generalist approach in addressing deepfakes issues was documented in a report produced by the European Parliament.

The EU's attempt to regulate deepfakes through the EU AI Act is worth noting. The Act does not propose an outright ban on the use of deepfake technologies, but it does impose "transparency" obligations on the creators of deepfake content. Article 52 (3) determines that *"users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated"*.

It is important to note, however, that the EU AI Act is still not approved. It should be approved by the end of this year and be enforced only by the end 2025.

UK

The UK hasn't approved yet any horizontal legislation banning the creation or distribution of deepfakes. The recently approved Online Safety bill criminalizes the sharing of deepfake content, but limits the prohibition to pornographic content only.

US

There are a handful of states in the US that have already passed laws regulating deepfakes. Virginia regulates pornographic deepfakes, while California and Texas laws cover disinformation intending to influence election results.
There is no regulation approved at the federal level, but 2023 has shown signs that this may change:

- Rep. Yvette D. Clarke re-proposed the “DEEP FAKES Accountability Act”. The main proposal of the bill is that deepfakes bear watermarks or identifying labels. The bill has not been voted on yet, and there are no current expectations of when it will be.
- The Federal Election Commission began efforts to regulate AI-generated content in the context of the incoming 2024 presidential election.
- In October 2023, a bipartisan group of senators (Coons, Blackburn, Klobuchar and Tillis) proposed a draft bill called the "Nurture Originals, Foster Art, and Keep Entertainment Safe Act" (NO FAKES Act). The bill is yet to be introduced but would propose:
    1. Introducing the concepts of "digital replica" (which covers deepfakes) and "digital replication right" (i.e. the right of the individual to authorize the use of the image, voice or visual likeness of the individual in a digital replica).

US

2. Holding individuals and companies liable for the reproduction of “unauthorized digital replicas”.
3. Holding platforms liable for disclosing “unauthorized digital replicas” if the platform knows that the content is indeed an “unauthorized digital replica”.

AI will be a key focus of regulations in 2024, and companies should take note with the understanding that AI safety is set to become an integral part of their activities.

Natalia Fritzen

AI Policy and Compliance Specialist, Sumsub

Actions like President Biden's Executive Orders and the UK government-sponsored AI Summit constitute important milestones for the AI industry, but they are not yet a 'finish line', especially when it comes to the regulation of AI technologies.

Until now, the United States treated guidance for the use of AI as exactly that—recommended guidance. And even Biden's Executive Order doesn't mean enforced regulation. Besides, it applies primarily to the US federal agencies, generating only indirect obligations to private actors. This laissez-faire approach to regulation differs from what other parts of the world are doing. The European Union, for example, is set to approve in 2024 the EU AI Act, the first comprehensive regulation on AI. The Chinese government has had a more hands-on approach as well, issuing regulations even on specific uses of AI, such as deepfakes.

As to the United Kingdom, what we see is an attempt to tackle forward-looking, more daunting topics, like frontier AI and AI existential risk, as seen at AI Summit. However, we need to first address existing issues such as AI bias or discrimination before we even think to solve the others. Coming out of the Summit, we need to walk the fine line between future and existing issues if we hope to truly shape AI governance.

Identity fraud forecast for 2024

Looking ahead to 2024, we expect certain developments in identity verification and fraud prevention.

Fraud landscape forecast:

1. **Deepfake advancements**

   Deepfakes will become increasingly advanced and challenging to detect.

2. **Escalation of account takeover and money muling**

   The proliferation of bought accounts and money muling schemes is expected to continue. Fraudsters will find innovative ways to exploit these tactics, necessitating more robust countermeasures and regulatory responses.

Preventive measures forecast:

1. **Stringent social network rules**

   The possession of identity data is projected to shift from global storage to being mandatory for local authorities. This change can enhance data security, privacy, and local control over sensitive personal information.

2. **Localization of identity data**

   The possession of identity data is projected to shift from global storage to being mandatory for local authorities. This change can enhance data security, privacy, and local control over sensitive personal information.

3 Mandatory local clouds

Localized cloud storage and processing are expected to become mandatory, bolstering data sovereignty and minimizing exposure to international data vulnerabilities.

4 Emergence of eID and video-based verification

Tighter regulations may drive the adoption of electronic identification (eIDs) or video-based identity verification with automated processes. This can offer enhanced methods for confirming individual identities.

5 Adoption of Web3 decentralized technologies

Web3 technologies and decentralized solutions may gain broader adoption, providing enhanced security and control over personal data in a decentralized digital landscape.

6 Non-document verification and alternative methods

There will be an increased emphasis on non-document verification and the adoption of alternative methods for identity validation, providing diverse and robust options for confirming identities.

7 Market consolidation

The identity verification and fraud prevention market is likely to witness consolidation as key players join forces to offer more comprehensive solutions.

8 Standardization of identity verification (IDV)

IDV processes will become more commoditized, simplifying and standardizing the way identity is verified across industries and platforms.

9 Network analysis in fraud prevention

Network analysis will become indispensable in efficiently combating fraud, allowing organizations to uncover complex patterns and connections that are indicative of fraudulent activities.

10 All-in-one KYC providers

KYC (Know Your Customer) providers are expected to evolve towards all-in-one solutions, offering a comprehensive suite of services for identity verification and fraud prevention.

Ilya Brovin

Chief Growth Officer, Sumsub

The main reason for using narrow-point solutions is the fact that customers have built in-house orchestration systems to allow them to work with multiple point solutions. This means point solution providers cannot give to the client a 360-degree view of the user, requiring the client to invest significant resources into keeping up with the technological advances of bad actors.

I hope to see that, in 2024, even large companies with resources to build their in-house onboarding orchestration systems realize that the resources and knowledge they employe at this stage is better dedicated to their core business and they start using outsourced platform solutions, which can do a much better job at catching fraud and monitoring the whole user lifecycle. One catalyst for this can be the continued improvement in AI technology which would vastly outpace the efficiency of internally-built systems.

How to fight identity fraud

A significant challenge faced today is the occurrence of identity fraud across the entire user lifecycle. Genuine users can pass initial verification but later engage in fraudulent activities. There's also the risk of legitimate users bypassing KYC for fraudsters' gain.

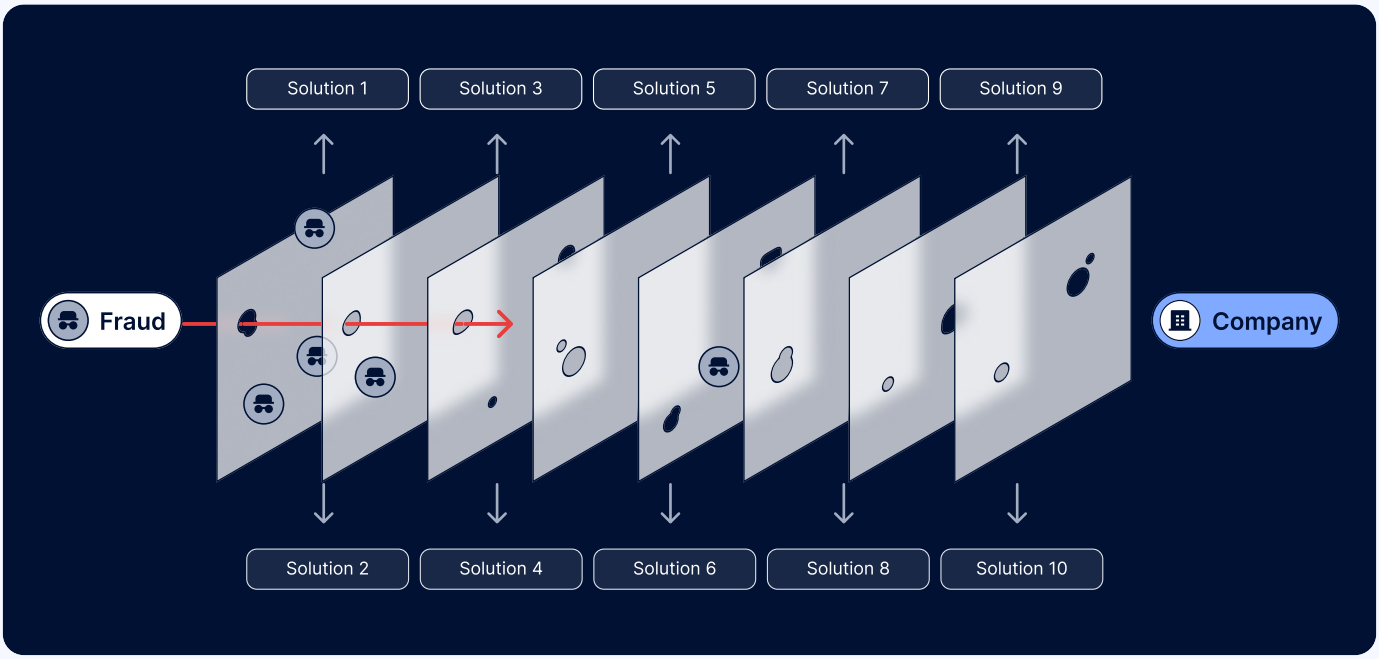
Andrew Sever

Co-founder and CEO of Sumsub

Our internal stats show that **an alarming 70% of fraud activity occurs past the KYC stage**, a clear indication for our business to adapt, as KYC checks alone are no longer sufficient.

To address this challenge, companies need to implement a multilayered approach that allows them to secure the whole customer lifecycle. This could involve the use of advanced authentication methods (such as biometrics or multi-factor authentication) to secure access to accounts, real-time monitoring for suspicious activities, regular employee training and awareness programs, and strong encryption for sensitive data.

The strength of such an approach lies in providing redundancy and diversity in security, ensuring protection even if one layer is breached. This approach makes it significantly harder for fraudsters to execute identity theft or fraud, as they must overcome multiple security barriers.



Frances Zelazny

Co-Founder and CEO of Anonybit

The proliferation of data has created troves of data that are nearly impossible to protect, as demonstrated by the continued drumbeat of data breaches. And it is the very data that is stolen from these data breaches that are used to pilfer account takeover fraud, having a significant impact on the bottom line. The fact is that 100% of fraud is happening inside KYCed accounts and 100% of fraud is also happening inside authenticated sessions.

It is time for a new approach that eliminates centralized data troves and leverages persistent biometrics across the identity management lifecycle—from digital onboarding to the point of service and account recovery—while eliminating the tradeoffs that are typically made between privacy, security, usability, and cost.

Checklist: How to prevent identity fraud

Preventing identity fraud for companies

1. Implement KYC protocols:

- ✓ Mandate robust Know Your Customer (KYC) procedures for client onboarding
- ✓ Regularly update and validate customer data
- ✓ Utilize identity verification services to cross-check client details
- ✓ Invest in technology that can identify deepfake videos and audios

2. Secure data storage:

- ✓ Use encryption for sensitive data
- ✓ Regularly update and back up databases
- ✓ Limit access to sensitive information

3. Implement strong authentication methods:

- ✓ Use multi-factor authentication (MFA) for accessing company systems
- ✓ Regularly update and strengthen password policies

4. Regular training & awareness programs:

- ✓ Educate employees about the latest fraud tactics
- ✓ Conduct regular cybersecurity drills

5. Monitor transactions:

- ✓ Implement real-time monitoring of transactions to spot suspicious activities
- ✓ Set up alerts for unusual patterns

Checklist: How to prevent identity fraud

6. Vet vendors:

- ✓ Ensure third-party vendors follow strict security protocols
- ✓ Regularly review and audit their security practices

7. Update security systems:

- ✓ Keep all software, especially security software, updated
- ✓ Regularly patch vulnerabilities in the system

8. Implement incident response plan:

- ✓ Have a plan in place for potential breaches
- ✓ Regularly review and rehearse the response plan

9. Employ physical security:

- ✓ Ensure secure access controls to company premises
- ✓ Use surveillance systems like CCTV cameras

10. Perform regularly audit & review:

- ✓ Conduct security audits regularly
- ✓ Review and update security policies as needed

11. Get feedback:

- ✓ Encourage employees to report suspicious activities
- ✓ Create an anonymous reporting system if necessary

For employees

1. Protect personal information:

- Don’t share personal details on public platforms
- Regularly review and clean up social media profiles

2. Be wary of unsolicited contacts:

- Don't answer unsolicited calls or emails asking for personal information
- Always verify the identity of the requester

3. Secure devices:

- Use strong, unique passwords for all accounts
- Install and regularly update antivirus software

4. Learn to spot deepfakes:

- Educate yourself on the characteristics of deepfakes
- Be skeptical of unexpected videos or audios from familiar figures, especially if the content is suspicious or controversial

5. Protect physical documents:

- Store important documents in a secure place
- Shred unnecessary documents that contain personal details

6. Monitor personal accounts:

- Regularly review bank and credit card statements for suspicious activities
- Check credit reports periodically

7. Use secure networks:

- Regularly review bank and credit card statements for suspicious activities
- Check credit reports periodically

8. Be cautious with emails:

- Don't click on suspicious links or download attachments from unknown sources
- Use spam filters to reduce phishing attempts

9. Stay informed:

- Stay updated about the latest fraud schemes
- Attend all cybersecurity trainings provided by the company

10. Lock devices:

- Use biometrics or PINs to lock personal devices
- Log out from applications or websites after use

11. Report suspicious activities:

- If you spot anything unusual related to your personal data or finances, report it immediately

Luke Raven

Fraud and Financial Crime Expert

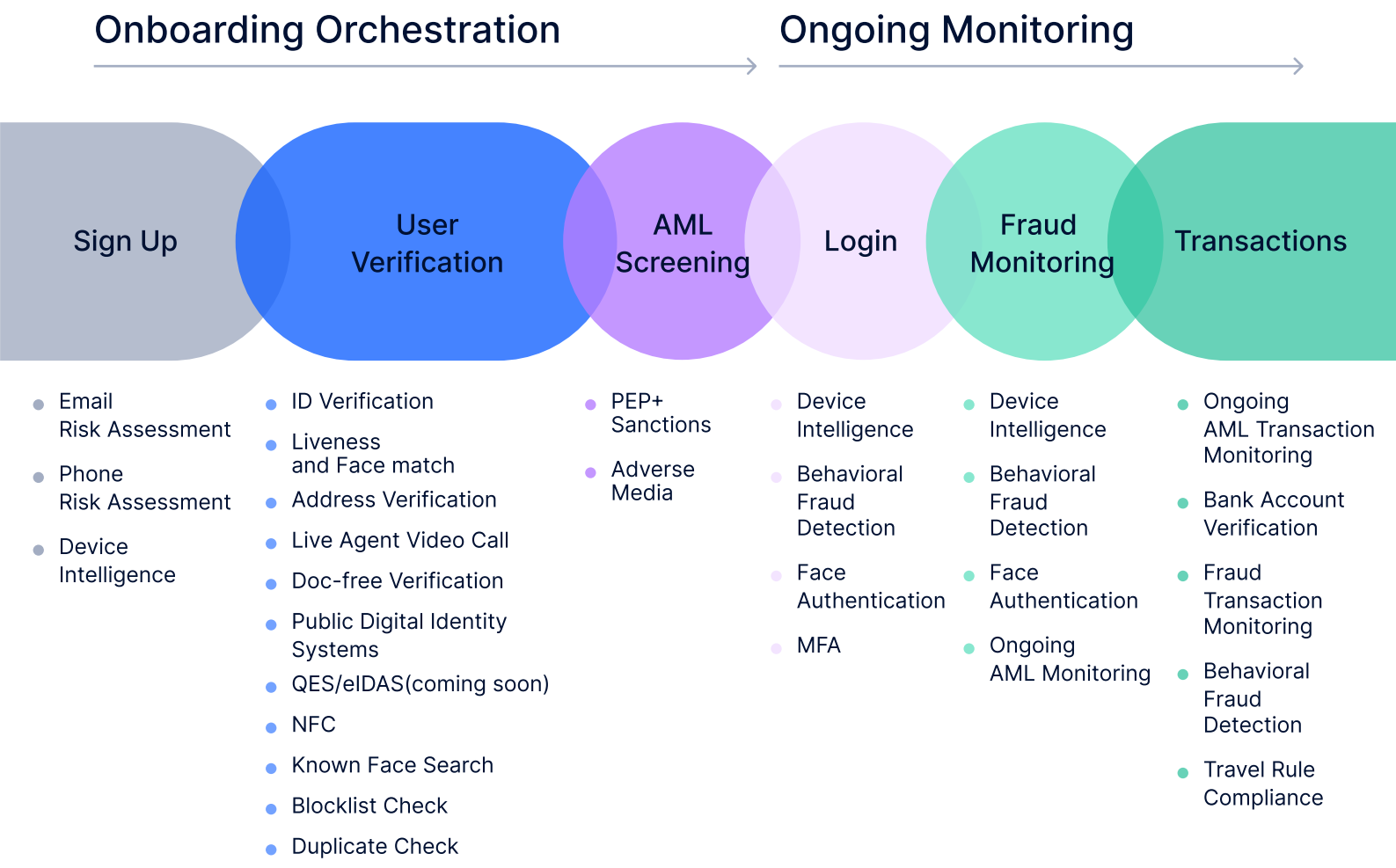
One of the ways to combat fraud is through a well-designed training program. By incorporating frequent (but fun!) testing exercises like phishing tests and celebrating wins in public, companies can foster a culture of awareness and vigilance. Sharing knowledge through lunch-and-learns with the fraud team can empower others and ignite their interest in fraud prevention.

How to combat fraud with Sumsub

Sumsub covers the whole user journey, from onboarding to transactions.

These include a wide range of verification solutions, including ID and Address Verification, Non-Doc Verification, AML Screening, Fraud Monitoring, and more.This comprehensive approach goes beyond the onboarding stage only, enabling entities to detect and prevent fraud at every step of the user lifecycle.

One verification platform to secure the whole user journey



Sumsub's fraud prevention system is based on a multi-layered approach that ensures the highest possible level of protection against all types of identity fraud, including the most advanced methods.

The system is powered by advanced AI with years of training data. Every single fraud countermeasure has been developed in-house by industry experts—and we constantly monitor the fraud landscape and update our systems to stay ahead of even the most sophisticated and modern fraud attack vectors.

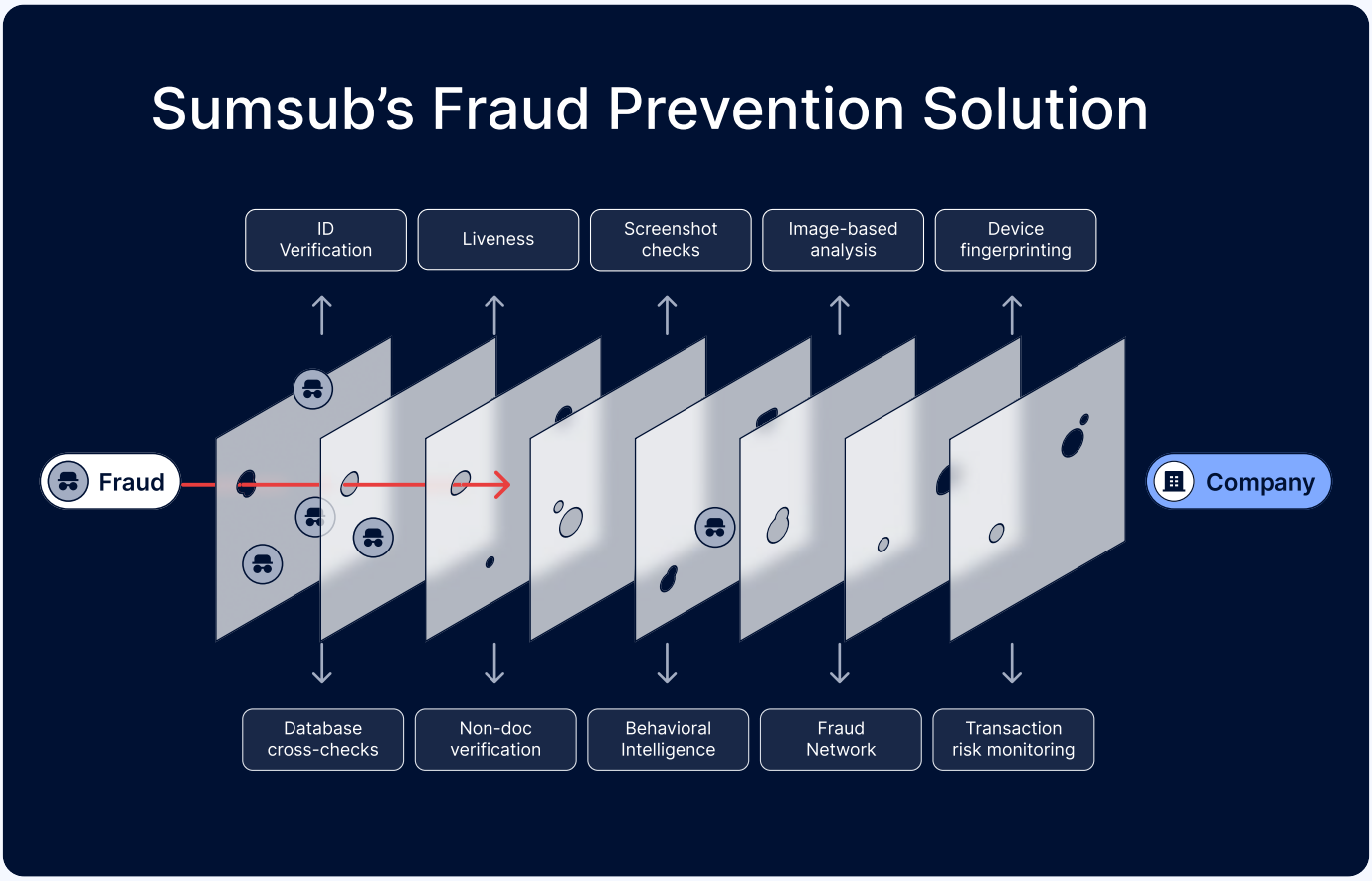
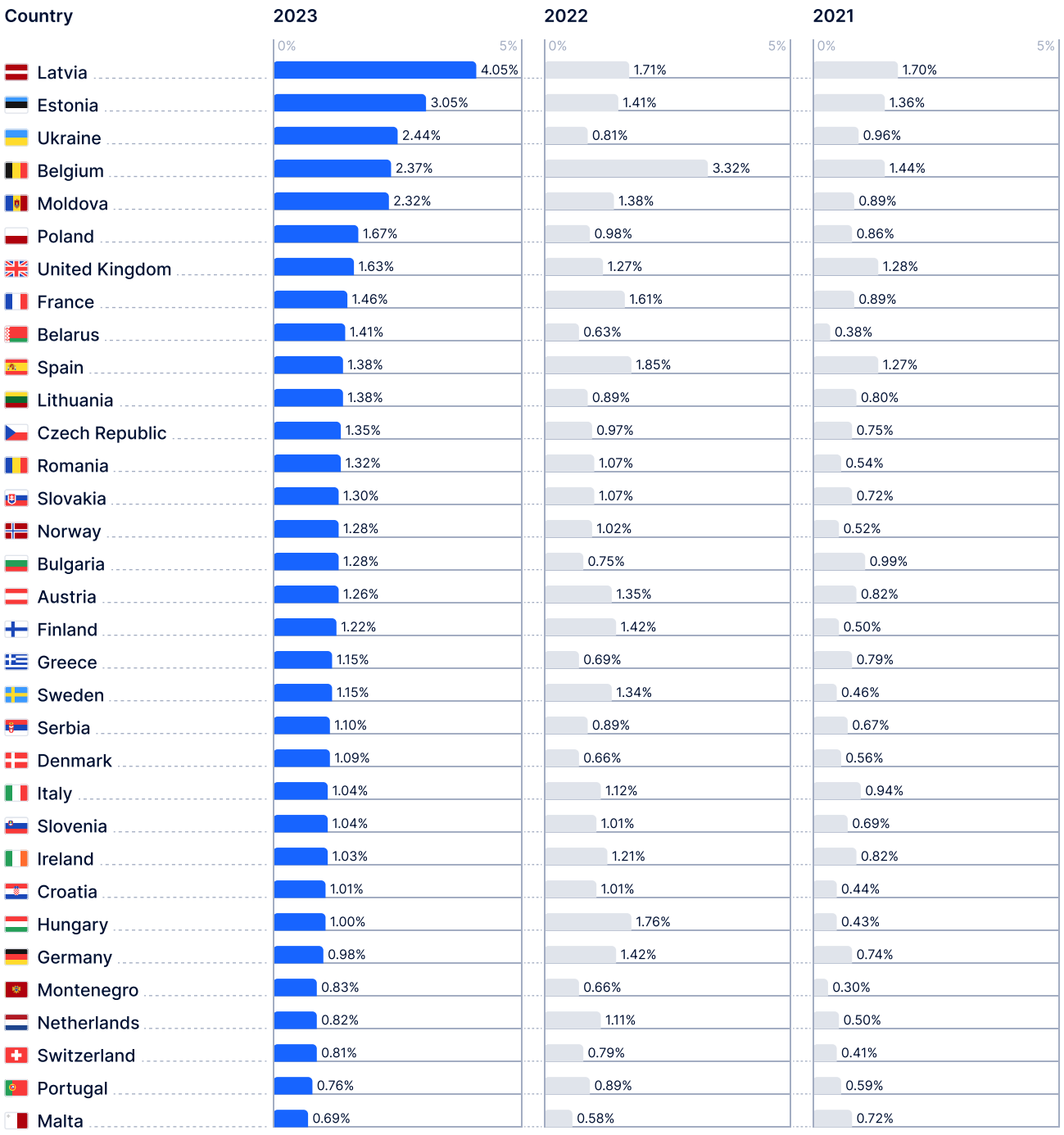


Chart 1. Identity fraud rates in Europe, 2021-2023



% of fraud in all analyzed verification by country

Chart 2. Growth in the number of deepfakes in Europe, 2022–2023

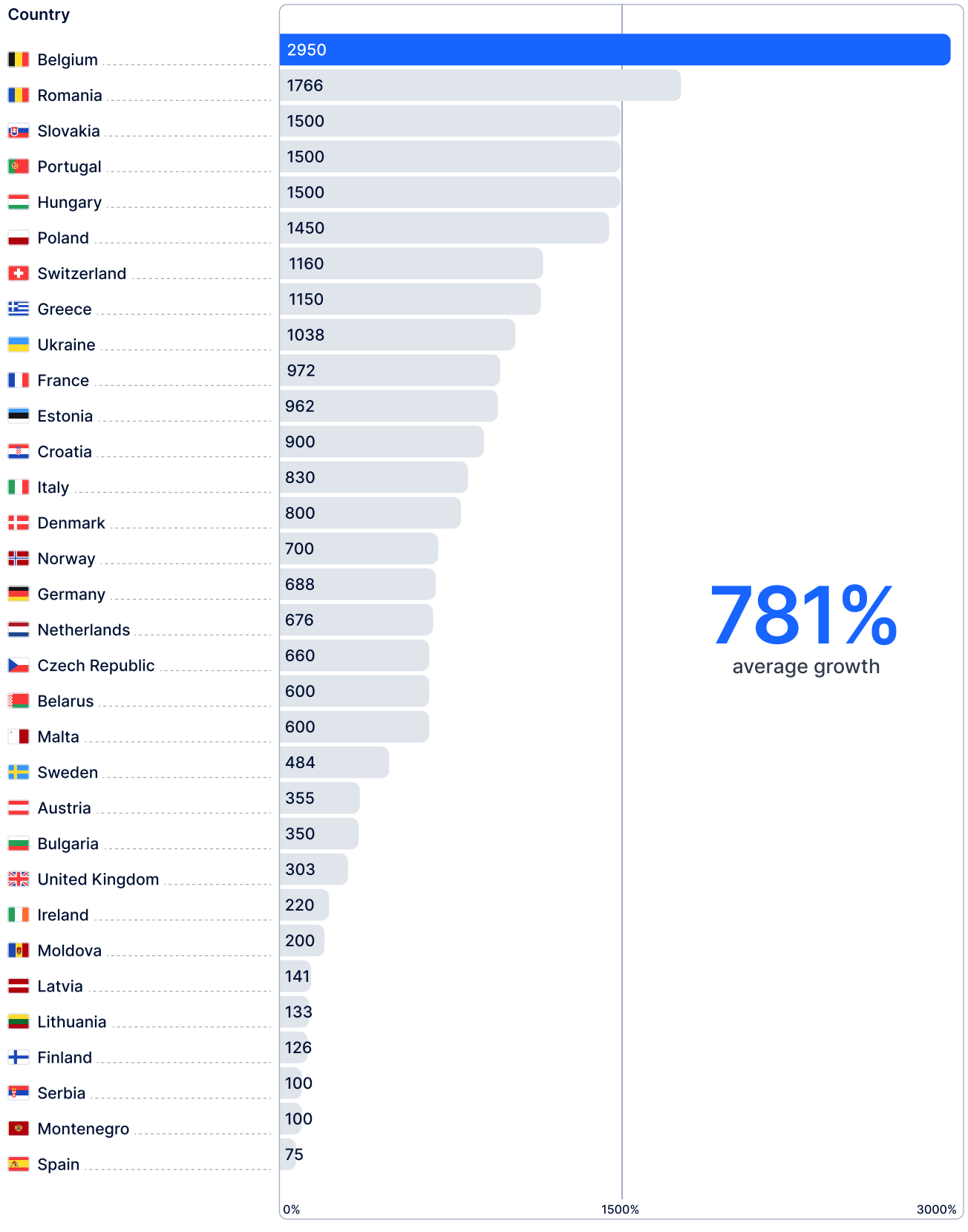


Chart 3. Growth in the number of deepfakes in APAC, 2022–2023

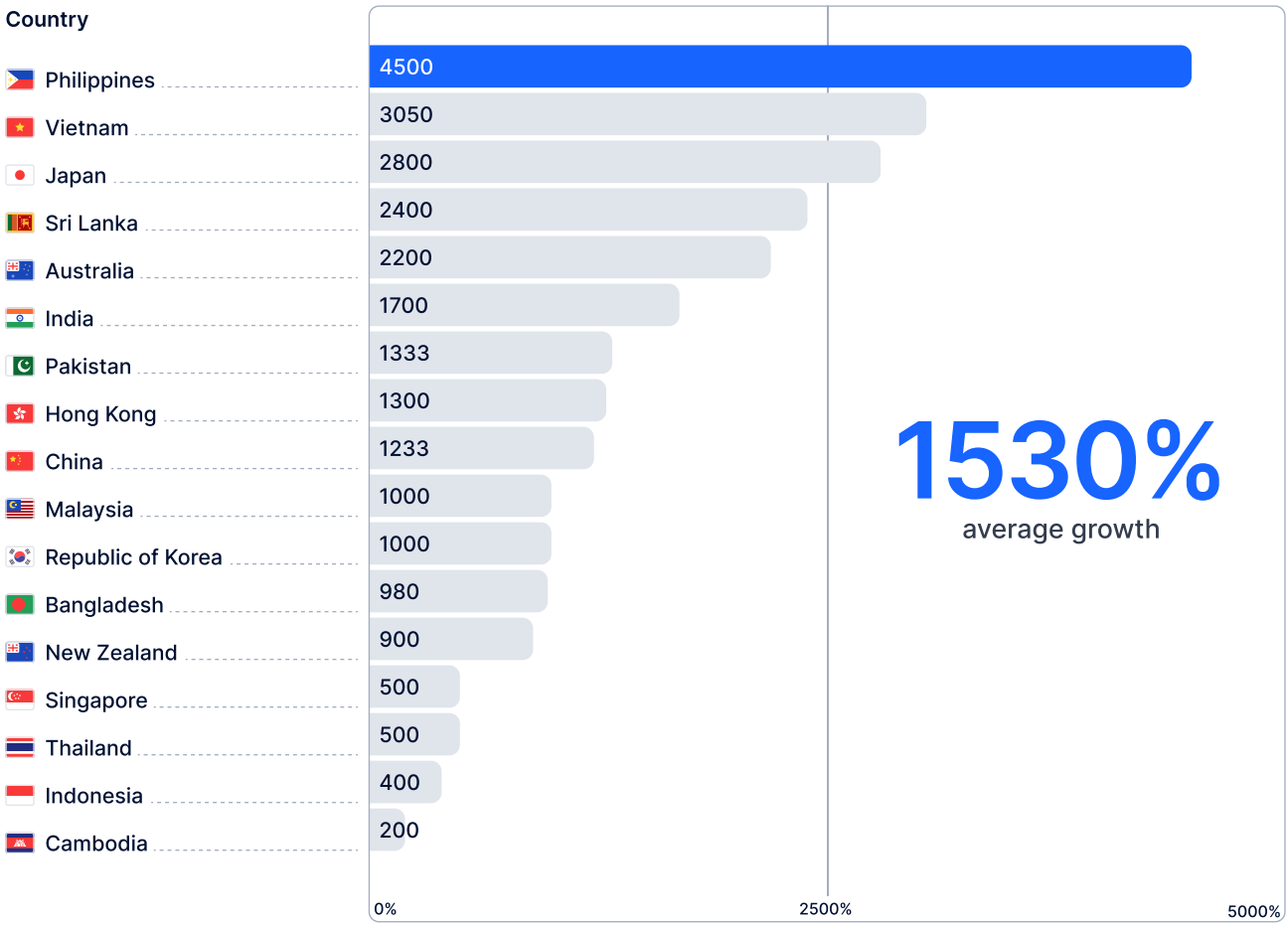


Chart 4. Growth in the number of deepfakes in MEA, 2022–2023

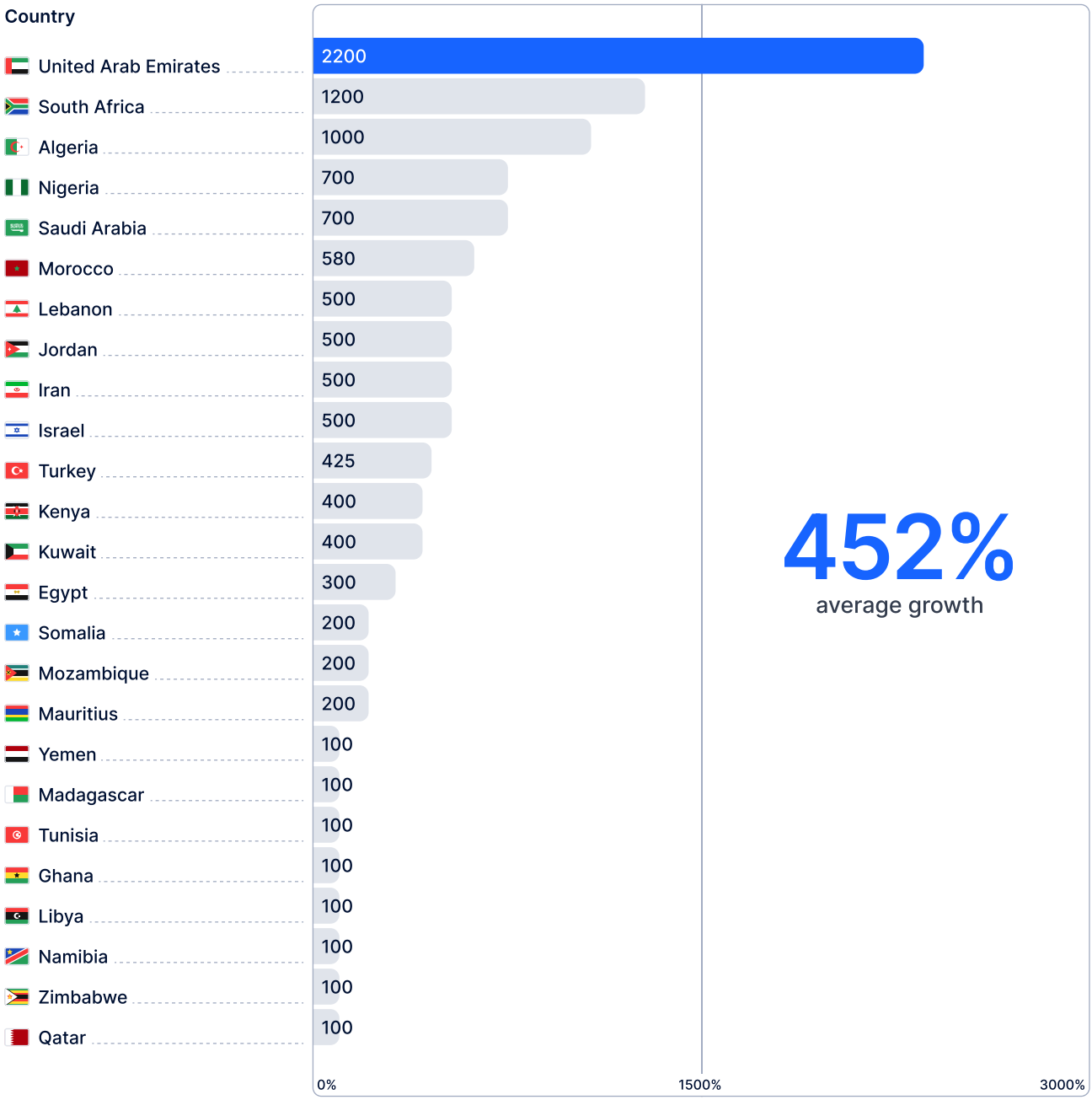


Chart 5. Growth in the number of deepfakes in LATAM, 2022–2023

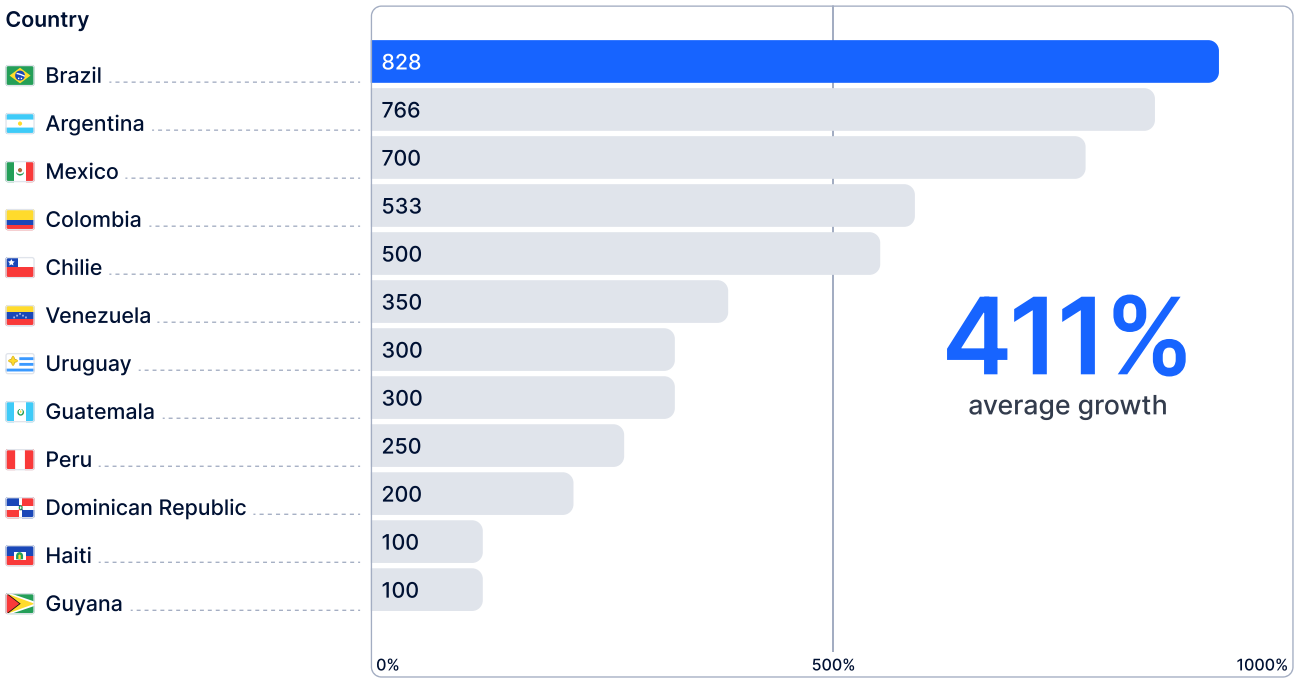
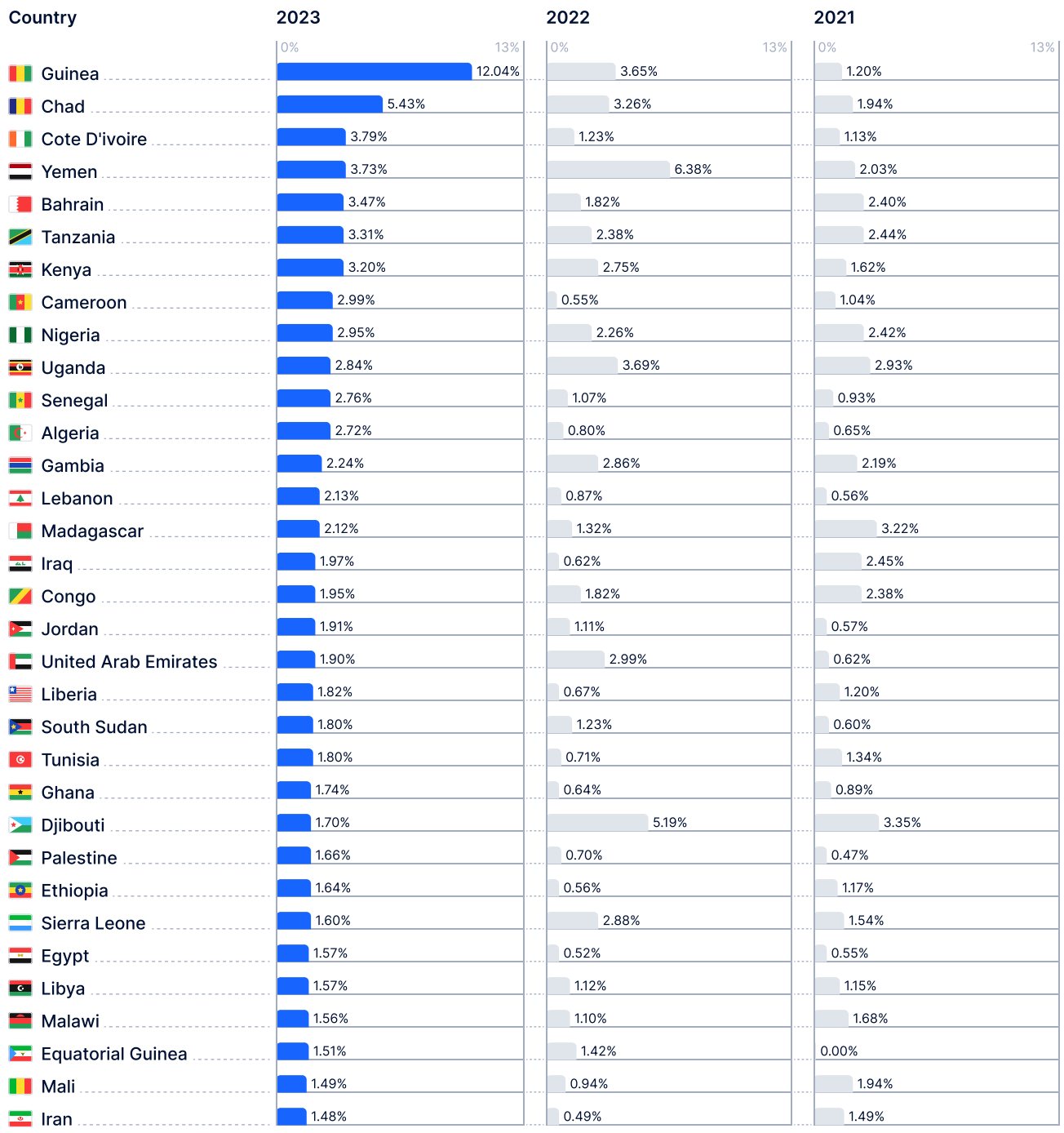


Chart 6. Identity fraud rates in Middle East and Africa, 2021–2023, part 1

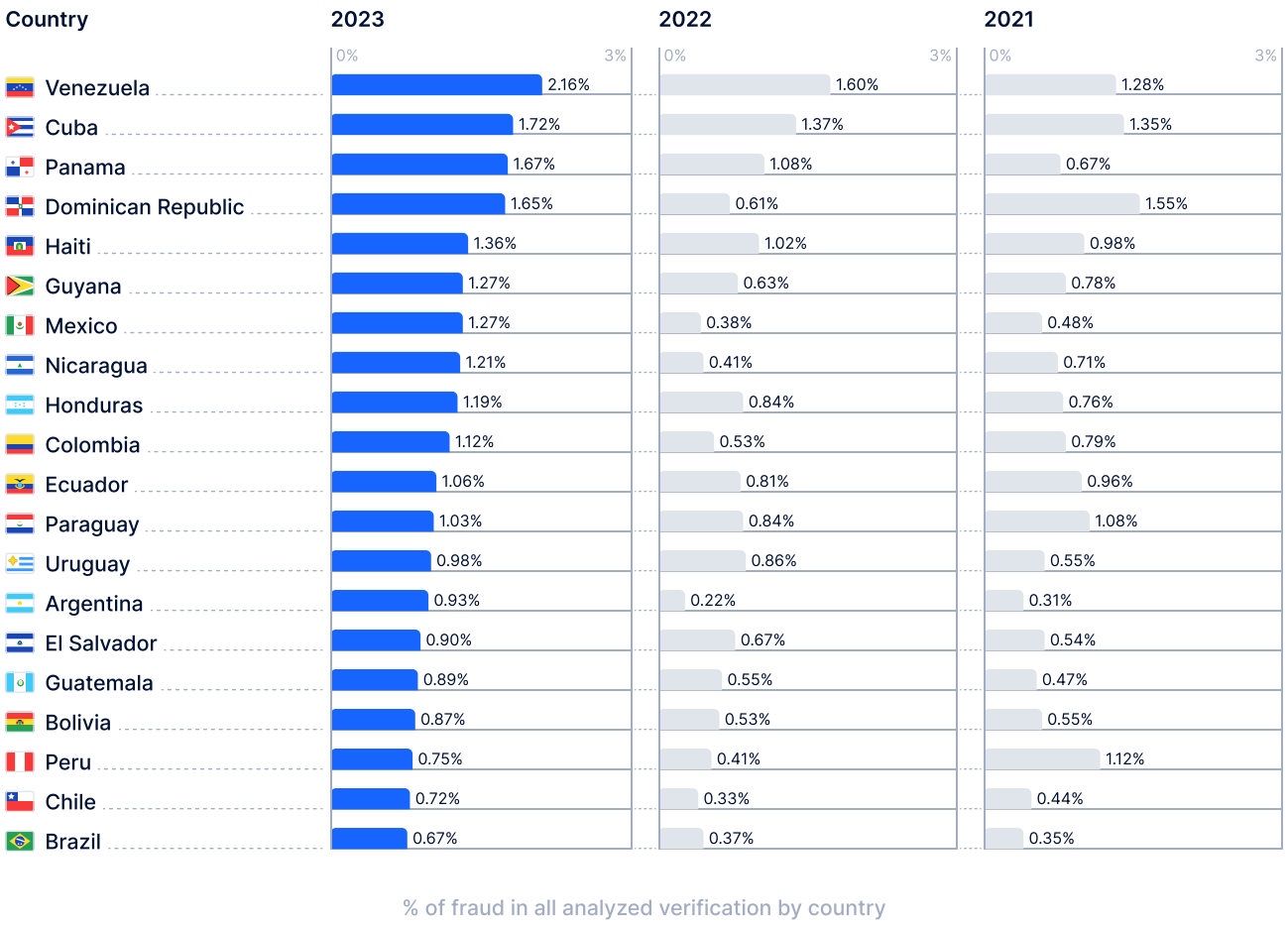


% of fraud in all analyzed verification by country

Chart 6. Identity fraud rates in Middle East and Africa, 2021–2023, part 2

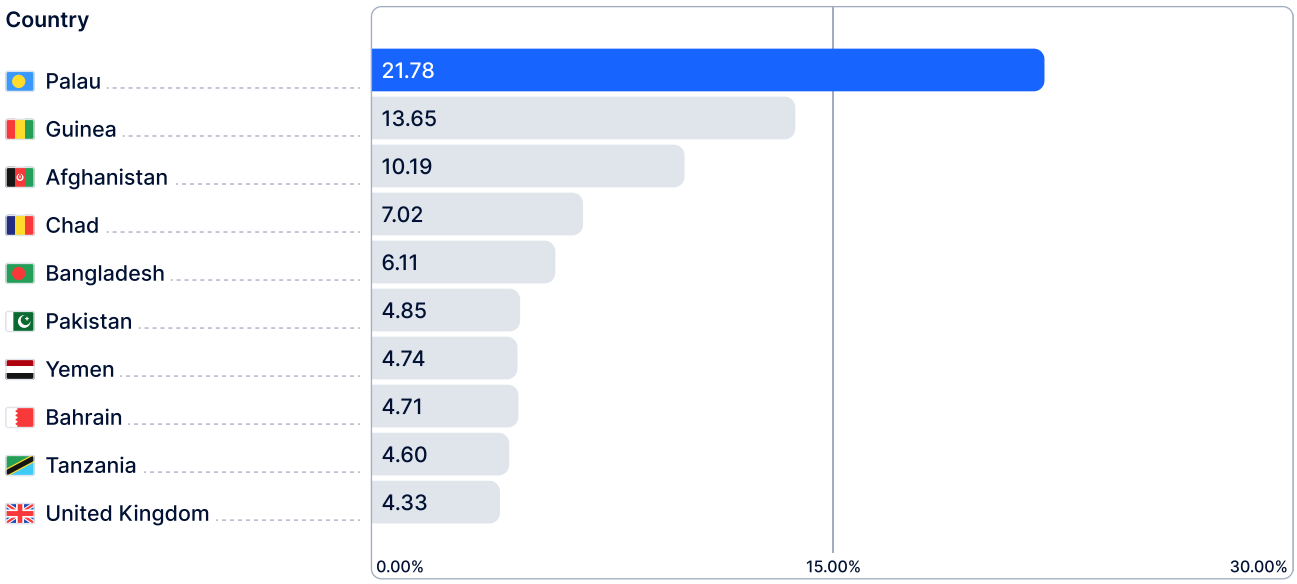
% of fraud in all analyzed verification by country

Chart 7. Identity fraud rates in Latin America, 2021–2023



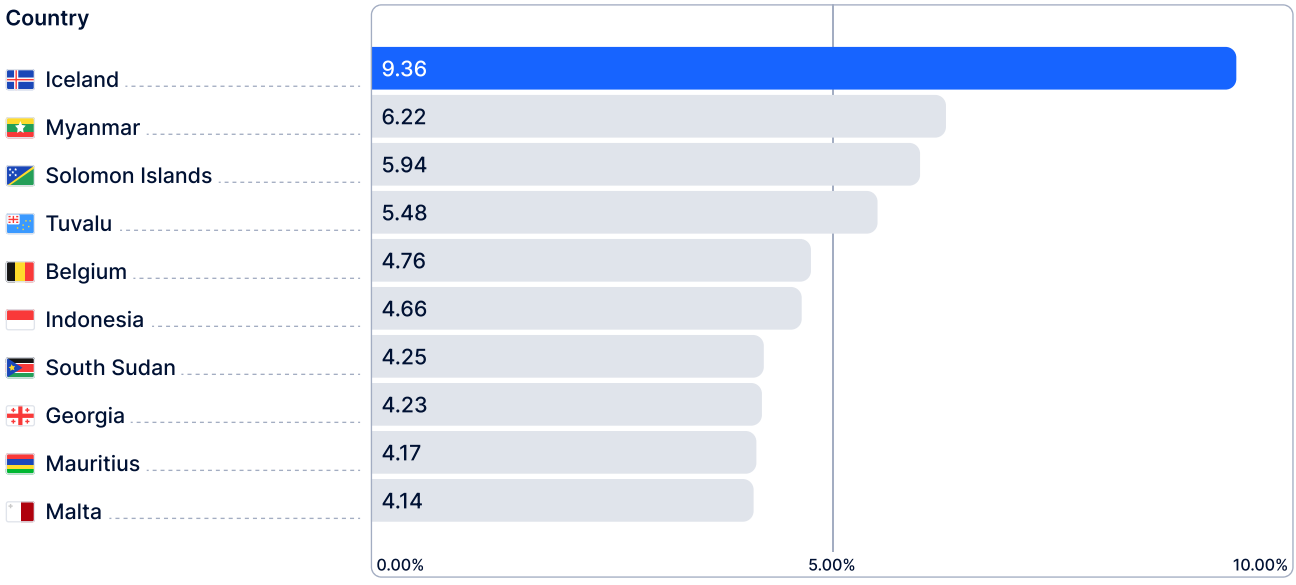
% of fraud in all analyzed verification by country

Chart 8. Top 10 fake ID Cards by country in 2023



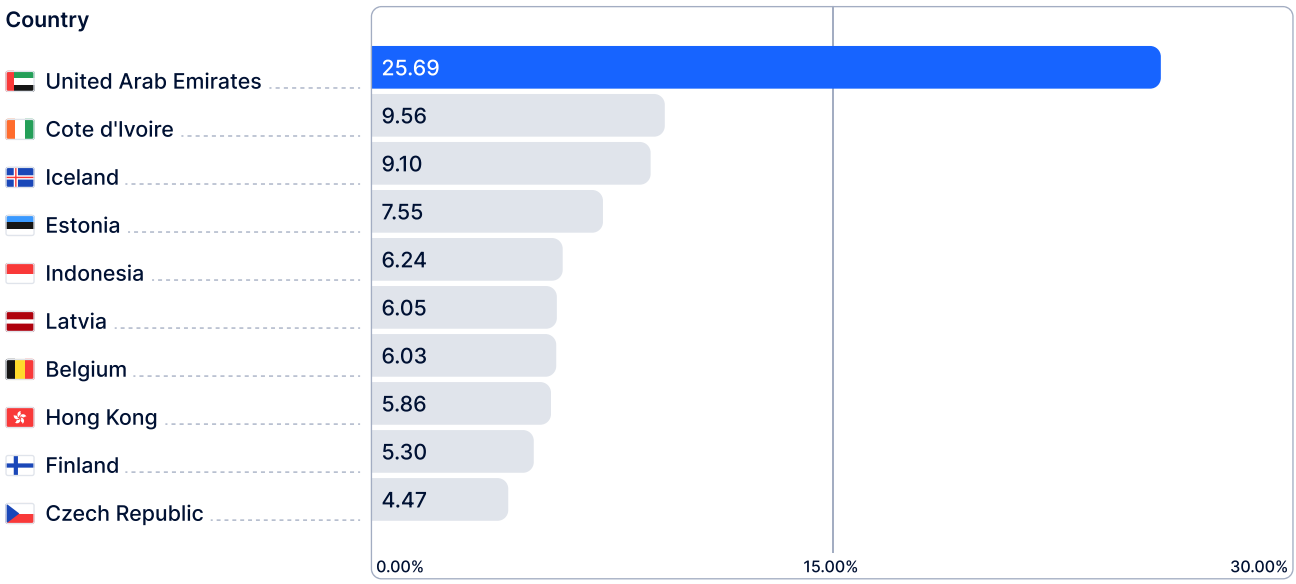
% of fraud in all analyzed verification by country

Chart 9. Top 10 fake driver licences by country in 2023



% of fraud in all analyzed verification by country

Chart 10. Top 10 fake national passports by country in 2023

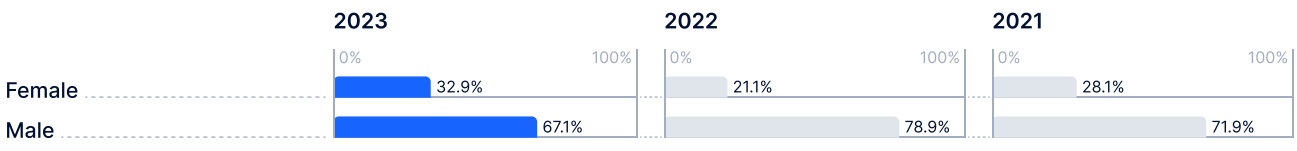


% of fraud in all analyzed verification by country

Notable statistics

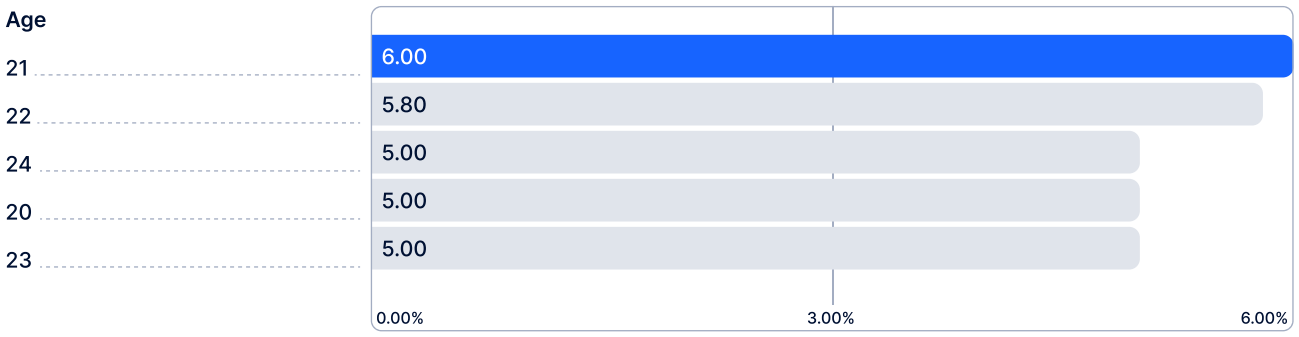
Thank you for reading our report to the end. Here you will find some more interesting statistics.

Share of fraudulent accounts by gender



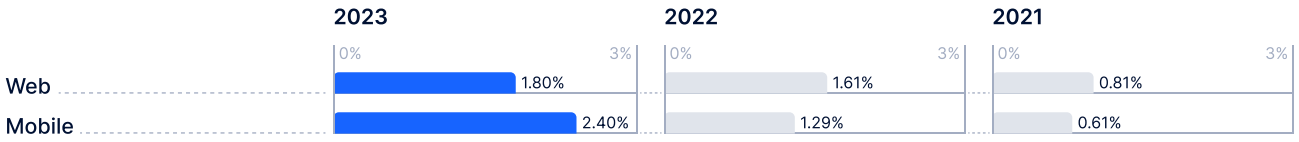
% of fraud in all analyzed verification by platform

Identity fraud in 2023 by age



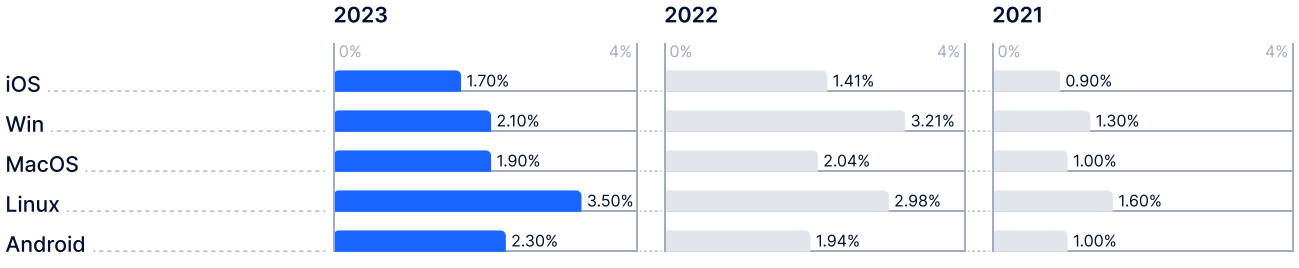
% of fraud in all analyzed verification by age

Identity fraud in 2023: Website vs Mobile app



% of fraud in all analyzed verification by platform

Identity fraud in 2023 by Operation System



% of fraud in all analyzed verification by OS

Want to stay fraud-free while keeping pass rates high?

Book a demo →

sumsub

www.sumsub.com