



sumsub



CryptoUK

State of Verification and Monitoring in the Crypto Industry 2023

A data-driven report on regulations and verification practices for crypto companies





1. About this report	03
2. Methodology	04
3. Key Findings	06
4. Trends in crypto verification and monitoring, 2023	08
5. Verification insights and challenges for crypto companies	12
6. Verification performance statistics	16
7. Fraud statistics	24
8. Regulatory changes: Travel Rule expansion	32
9. Report Summary	35
10. How Sumsb can help	37



This comprehensive report looks into the latest insights, key practices, and statistics on identity verification in the crypto industry.

It provides crypto businesses with a clear understanding of industry verification standards and trends, offering ideas on how to enhance the user experience and improve operations.

The research was conducted by Sumsb, a tech company that helps businesses secure the whole user journey, offering one platform that includes User Verification, Business Verification, Transaction Monitoring, Travel Rule, and Fraud Preventions solutions.

! Please don't share the content of this report without giving us credit.
© Sum and Substance Ltd (UK), 2023

This study seeks to understand the verification practices of crypto businesses.

Main verification aspects considered

 Verification methods

 Speed of checks

 Pass rates

 Fraud cases

 Compliance



The three main sources of data used in this report

100+

crypto companies
surveyed

Millions

of verification
checks analyzed

800,000+

fraud attempts
studied

The methodology for this report consists of three main components



A survey conducted among 100+ crypto companies

to gather direct insights into their current practices and experiences with user verification. The survey questions covered various aspects of verification, such as onboarding processes, fraud prevention, and compliance measures.



Internal statistics and data were thoroughly analyzed

We considered the first 8 months of 2023 and compared our findings with the same period in 2022 identifying common verification patterns and challenges faced by crypto companies.



Expert interviews were conducted with professionals

in the crypto industry. This gave valuable insights on verification trends, regulatory changes, and potential solutions.

All graphs and infographics are based on internal statistics compiled from the data of customers who gave their consent, and a survey. The data has been aggregated and anonymized.

Key Takeaways

Numbers of 2023

<60 seconds

average
verification time
globally

21 seconds

average verification time in Germany,
one of the fastest regions for doc-
based checks

Challenges of the year



Fraud prevention

Fraud is becoming more
sophisticated



Travel Rule compliance

It's getting harder to meet
emerging regulatory
requirements

Threat technology of the year

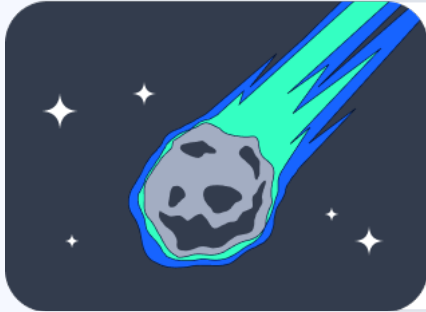


Deepfakes

In 2023, the number of deepfakes
in the crypto industry increased by

128.15% compared to 2022

Main trends in crypto verification for 2023



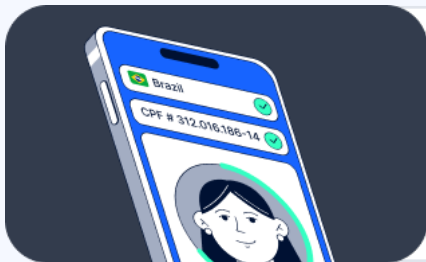
1

Fraud cases have decreased in number, but the attack methods are getting more professional.



2

The emergence of AI tools is giving rise to threats such as deepfakes.



3

The shift from document-based to doc-free verification solutions is underway.



4

Compliance measures have become increasingly widespread with the global implementation of the Travel Rule.



5

Legacy verification solutions are no longer sufficient in the face of increasingly sophisticated fraud threats.

Trends in crypto verification and monitoring, 2023

In 2023, the crypto industry continues to evolve and mature, becoming increasingly integrated into the mainstream financial system.



Dr. Zvi Gabbay



Senior Partner, Head of Capital Markets and Financial Regulation Department Barnea Jaffa Lande & Coin
an interview with the "Sumsup for Experts" YouTube channel

[the] Crypto industry is looking for bridges to connect to the conventional system, and these bridges can only be built if there is regulation.

- i** Governments and regulatory bodies around the world are actively working towards establishing a clear framework for cryptocurrencies*, which will provide greater clarity and stability for the industry.

* In this report, the terms "cryptocurrencies", "virtual assets" and "digital assets" are used interchangeably.

There's growing momentum to regulate crypto service providers

While many countries have Anti-Money Laundering (AML) rules, not all apply them to crypto providers yet. This is driven by the need to address concerns around growing fraud, illicit activities, and bankruptcies specific to the crypto space. Meanwhile, the FATF Travel Rule is embraced by more and more countries, with UK as a recent add-on.



Tony Petrov

Chief Legal Officer at Sumsu



A lack of AML & KYC controls can be an early warning sign that an exchange or vendor may have fundamental problems... It can be expected that this component will become the number one due diligence item for venture funds investing in crypto fintechs.

This year's significant regulatory developments in the crypto industry were marked by the Grayscale case. In August, Grayscale scored a legal victory against the U.S. Securities and Exchange Commission (SEC) in regards to its ETP application (spot bitcoin traded fund with freely tradable shares).

The outcome sets a precedent for crypto regulation in the US, shaping the future and highlighting the need for comprehensive regulatory frameworks that provide clarity for market participants and investors.

Web3 compliance trends

The trend toward collaboration between regulatory bodies and crypto is further underscored by the transformative potential of Web3, where regulatory frameworks will be essential to navigate the challenges and opportunities presented by decentralized technologies.



David Zareh

OnChain Accounting



"Web3 is poised to significantly reshape compliance across various sectors. Enhanced data privacy, security compliance, and the management of decentralized financial transactions, especially concerning cryptocurrencies and DeFi platforms, will necessitate the development of robust regulatory frameworks.

Intellectual property compliance will gain complexity with the rise of Non-Fungible Tokens (NFTs) and decentralized autonomous organizations (DAOs), requiring innovative strategies to safeguard creators' rights and ensure lawful operations. Furthermore, the globalization and decentralization inherent in Web3 will demand meticulous navigation through international regulations and tax obligations, ensuring adherence across diverse jurisdictions.

Therefore, a collaboration between regulatory bodies and organizations will be imperative to navigate the multifaceted challenges and harness the potential of Web3 effectively.

Fraud and other crime continue to be a prominent concern for the industry,

[including investment scams, ransomware, and more](#). However, for some of these challenges, countermeasures at the state level are gradually making criminals more vulnerable, as police and other authorities acquire new tools for investigations. For instance, in February 2023, [the Department of Justice \(US\) successfully located \\$3.6 billion worth of Bitcoin](#) that had been stolen back in 2016.

- i** Identity fraud remains a significant concern for crypto companies. Fraudsters continue using cutting-edge technologies, such as AI, to develop more sophisticated methods to deceive crypto companies.



Pavel Goldman-Kalaydin

Head of AI/ML at Sumsu



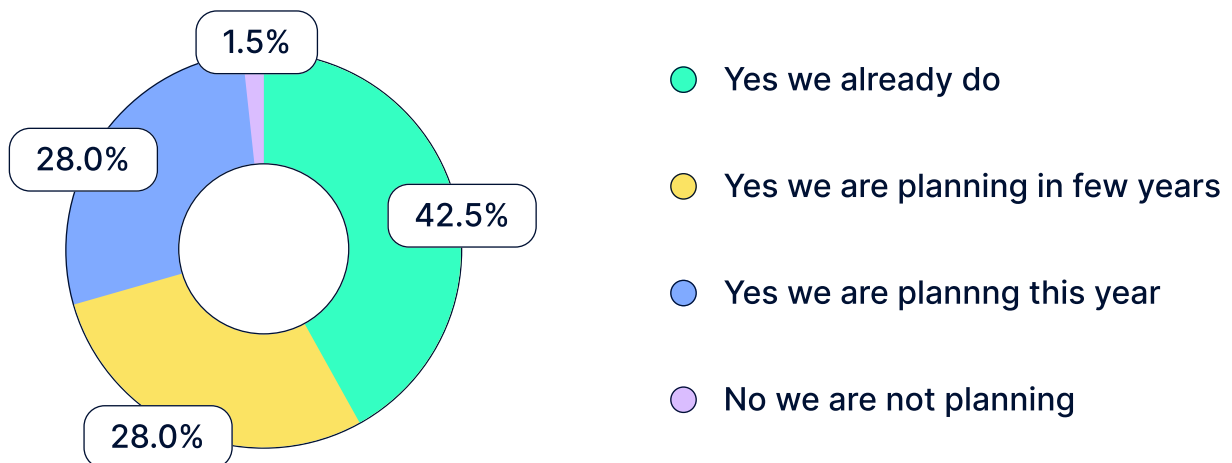
As we face the ever-evolving trends in generative AI and AI-driven fraud, we anticipate AI technologies to develop quickly, and more sophisticated fraud to emerge, affecting even more industries. The use of synthetic fraud is rising at an alarming rate and pioneering to the rapid spread of misinformation, as recently seen with the fake images of a supposed explosion at the Pentagon resulting in significant media hype.

Verification insights & challenges: crypto companies view

The main challenges that crypto companies face in 2023 are the spread of Travel Rule regulations and more advanced fraud methods.

Our data indicates that 98.5% of crypto companies already integrated or plan to integrate Travel Rule solution providers.

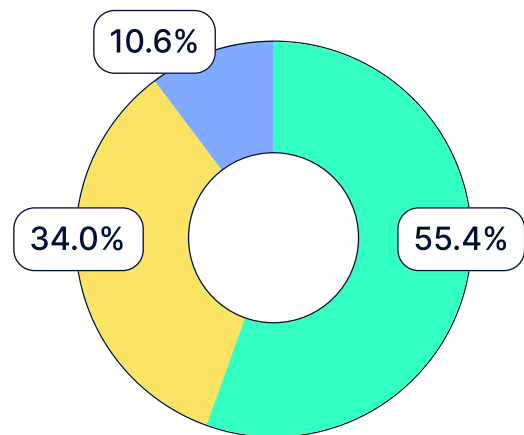
Do you plan to use a Travel Rule solution provider?



Our research reveals that 55% of crypto companies reported an increase in fraud-related losses connected to applicants. On the other hand, 34% stated that they noticed no change fraud-related losses this year.

Do you see any changes in fraud-related losses this year compared to previous years?

● Increase ● No change ● Decrease



7/10

Deepfakes are a growing concern for the crypto industry, with 70% of companies noting their increasing popularity among fraudsters. This matches our data that shows a shift from the use of expensive rubber masks to relatively cheap deepfakes by fraudsters.

77%

of crypto companies have observed new fraud patterns and schemes. Meanwhile, fraudsters are constantly devising new ideas to exploit vulnerabilities in the crypto industry.



Matthew Hogan

Expert in fraud investigations



In 2023, I've observed two significant fraud trends in cryptocurrency-related crimes.

First, there has been a substantial shift away from cryptocurrency kiosk-related crimes towards investment-style and pig butchering scams, likely driven by the rise of decentralized finance (DeFi) and increased anonymity in cryptocurrency transactions. These scams often involve scammers befriending victims on social media or dating apps and persuading them to invest in fraudulent cryptocurrency projects.

Secondly, the standardization of investment and pig butchering scams has become evident, with victims consistently reporting similar sequences of events. This standardization enables scammers to streamline their operations, making it easier to target more victims.

Looking ahead to 2024, I'm anticipating that these cryptocurrency fraud patterns will continue evolving, becoming more sophisticated and likely including more advanced AI and deepfakes.

Crypto companies mentioned various fraud schemes they faced for the first time this year, these included:

Case 1

AI-generated profiles

“I have seen 2 profiles which were made with the help of AI. An additional verification (manual) is required. The AI made all the smurfing in a way that it was difficult to recognise by software. The human effort should be very attentive to details. I used Google reverse image and tineye to detect the inappropriate/fraudulent act.”

Case 2

Crypto money muling

“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 the 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 first case shows that crypto companies are facing adverse effects of the AI technologies on their verification processes. This makes the industry seek more advanced anti-fraud solutions that allow AI-powered fraud to be detected automatically.

The second case highlights the importance of a comprehensive approach to fraud protection. Even with advanced deepfake detection systems, fraudsters can manipulate individuals who willingly undergo KYC verification. To effectively address this issue, a multi-layered approach that includes transaction monitoring and behavioral antifraud measures is crucial. At Sumsb, we use clustering algorithms to identify money mules and prevent them from extracting laundered funds.

Verification performance statistics: speed, pass rates, methods

Identity verification speed by region

Across all regions, verification time has nearly halved from 2022 to 2023

i Europe currently leads as the fastest region, with onboarding taking less than 30 seconds. Meanwhile, verification speed has increased by 1.75 times in Africa, 1.53 times in Asia, and 1.89 times in Latam.

Average time for standard user verification



Identity verification speed by country

In 2023, a significant decrease in average verification time was observed among Sumsb's crypto clients. Brazil (+65.4%), Mexico (+61.9%), and Germany (+58.0%) stand out as the top three countries with the most significant improvement in verification time. Germany is among the leaders with an average verification time of 21 seconds for the standard verification flow.



- i** In 2023, the average verification time takes less than 60 seconds worldwide.

* Standard verification flow stands here and later for ID+Liveness+ PEP, sanctions lists and adverse media checks

Average time for standard verification flow in crypto

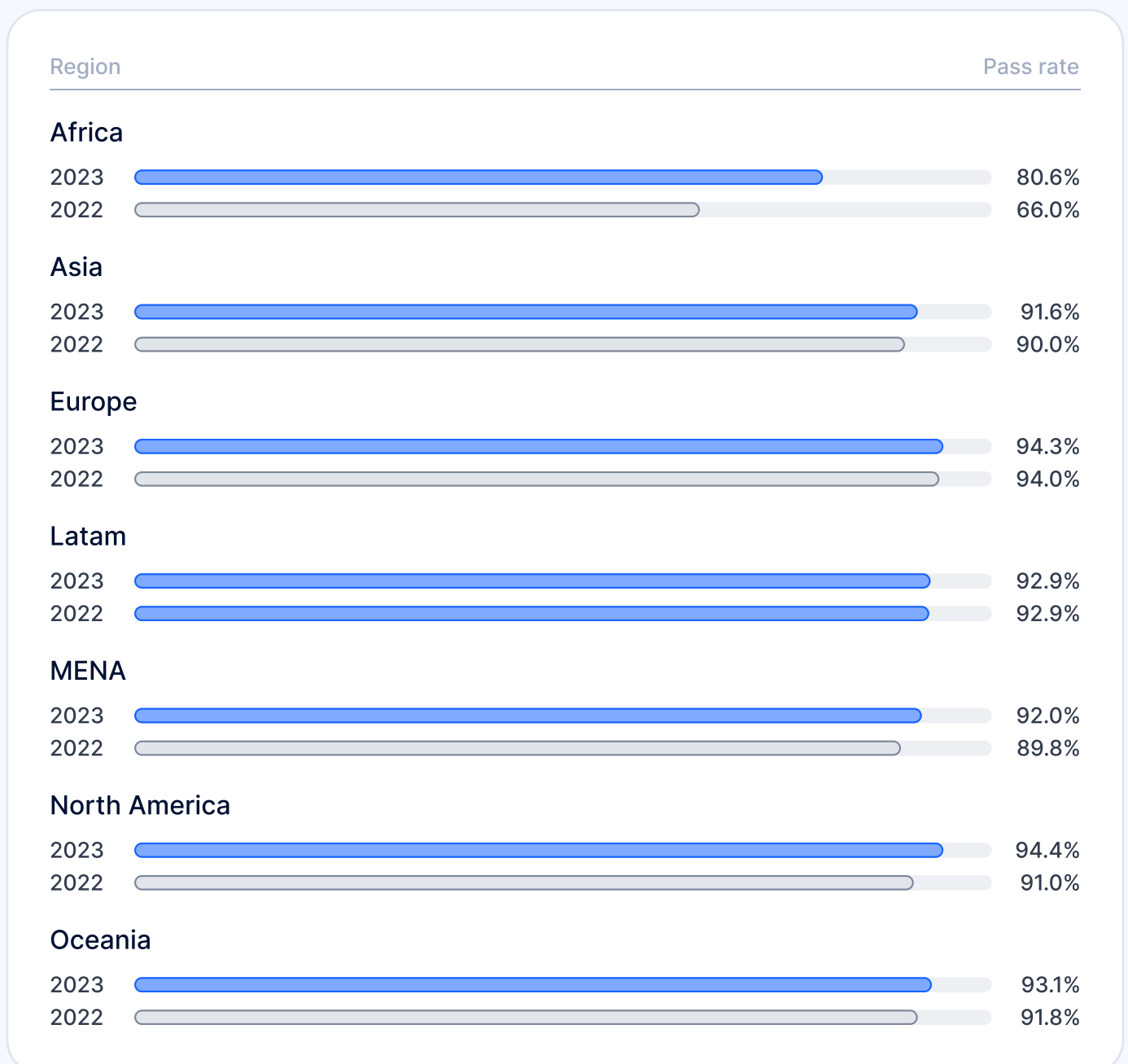


Identity verification pass rates by region

Africa has seen the largest increase in pass rates, but there is still room for improvement. With a relatively lower pass rate compared to Europe and North America, Africa's verification landscape may be influenced by factors like poor photo quality which depends on the devices used.

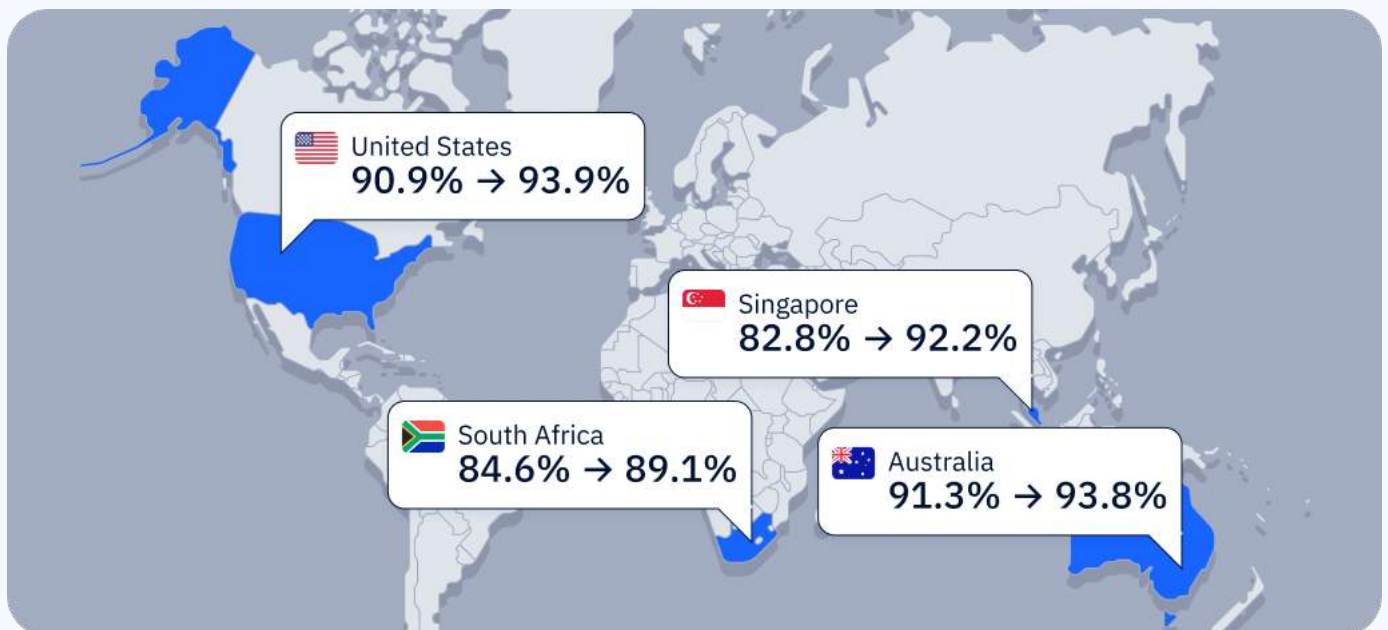
Meanwhile, the average pass rate in Europe and North America is high, at around 94%

Average pass rate for standard verification flow, by region



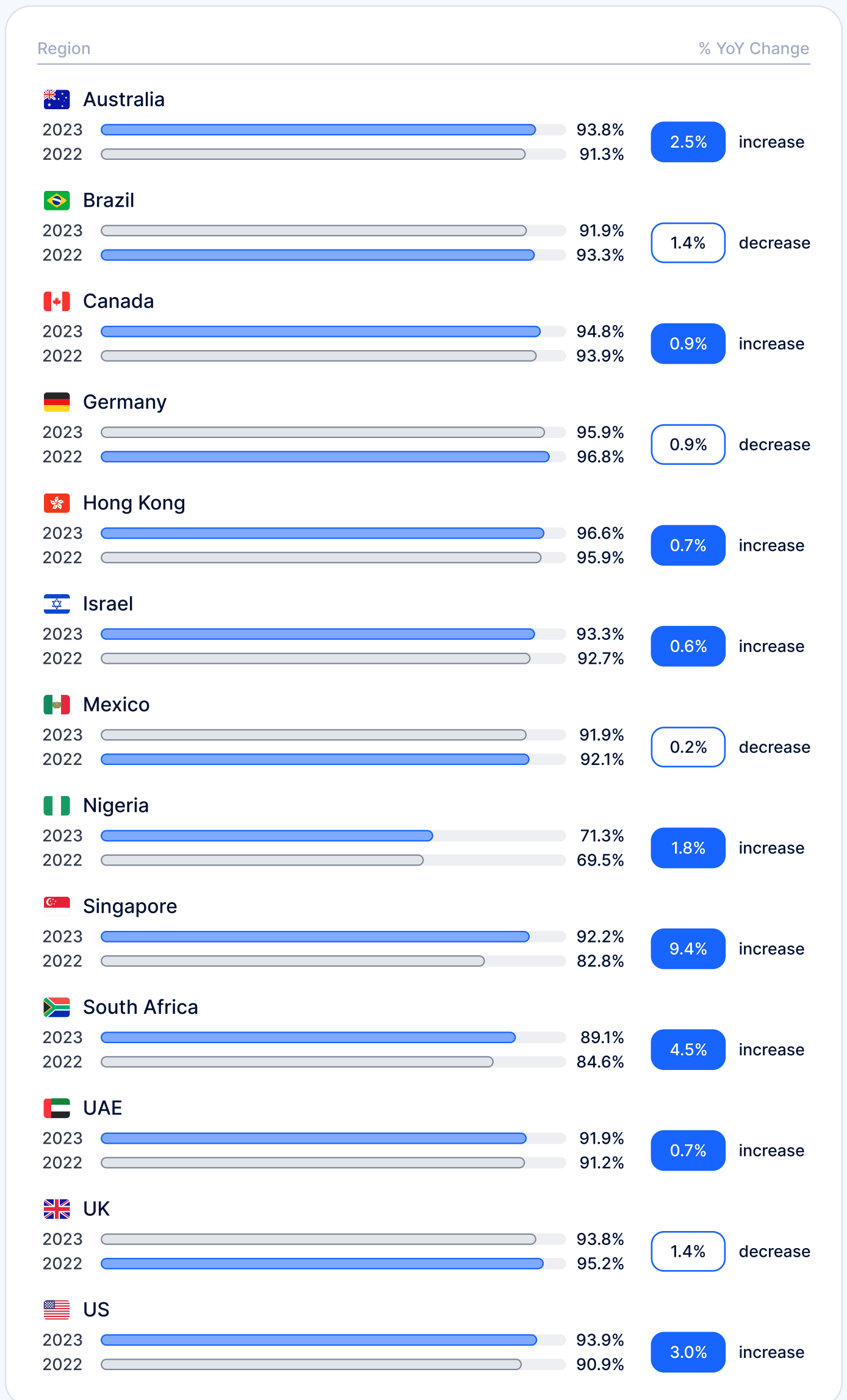
Identity verification pass rates by country

In 2023, the most substantial growth in average pass rates was reached by Singapore (from 82.8% to 92.2%), South Africa (from 84.6% to 89.1%), Australia (from 91.3% to 93.8%), and the United States (from 90.9% to 93.9%) experienced a significant increase as well.



Hong Kong has had one of the highest pass rates in 2023 with 96.6%

Average pass rates for standard verification flow, by country



Proof of Address verification pass rates by country

Proof of Address (PoA) verification can pose challenges for crypto companies as document types vary greatly across countries. This process can result in drop-offs as users face difficulties in submitting the required documents.

However, using a verification provider with advanced technical infrastructure and extensive experience in handling documents can help crypto companies achieve high pass rates.

In 2023 the highest conversion rates for PoA were achieved in Singapore (91.5%), Slovakia (89%), and Hong Kong (87.5%).

In 2022 Turkey (86.8%), Singapore (84.7%), and Canada (80.2%) were among the leaders based on PoA conversion rates.



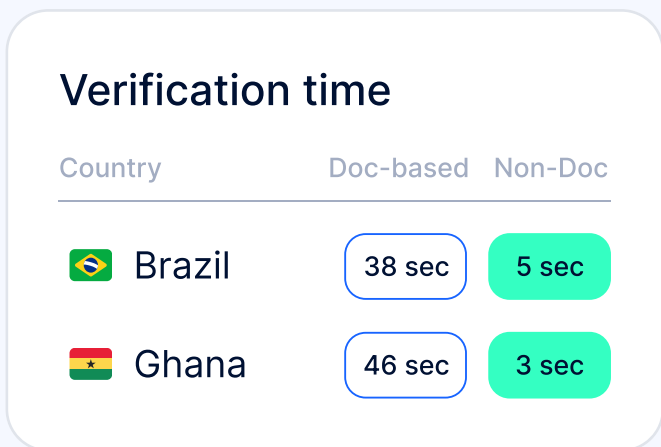
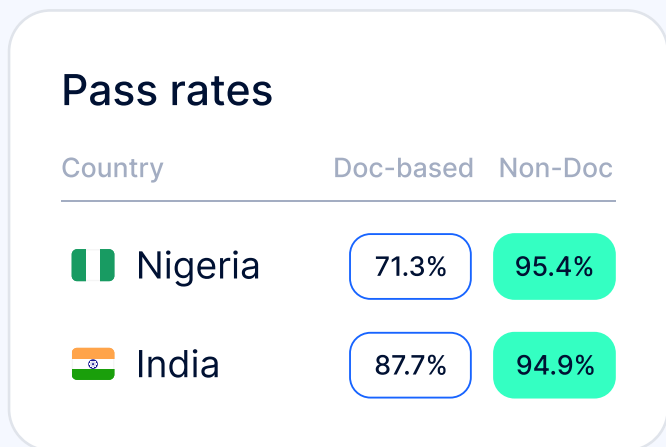
Non-Doc Verification statistics

Non-Doc Verification uses government databases where regulations permit. This method gained more popularity last year, making onboarding faster and more user-friendly. Additionally, the use of such databases makes fraud almost impossible since the information is pre-verified by governments.

At Sumsb, Non-Doc Verification is available in 9 countries: Argentina, Bangladesh, Brazil, Ghana, India, Indonesia, Nigeria, Netherlands, and the UK.

Implementing Non-Doc verification has allowed us to achieve impressive pass rates and dramatically reduce verification time. Below are Sumsb’s 2023 Non-Doc Verification results:

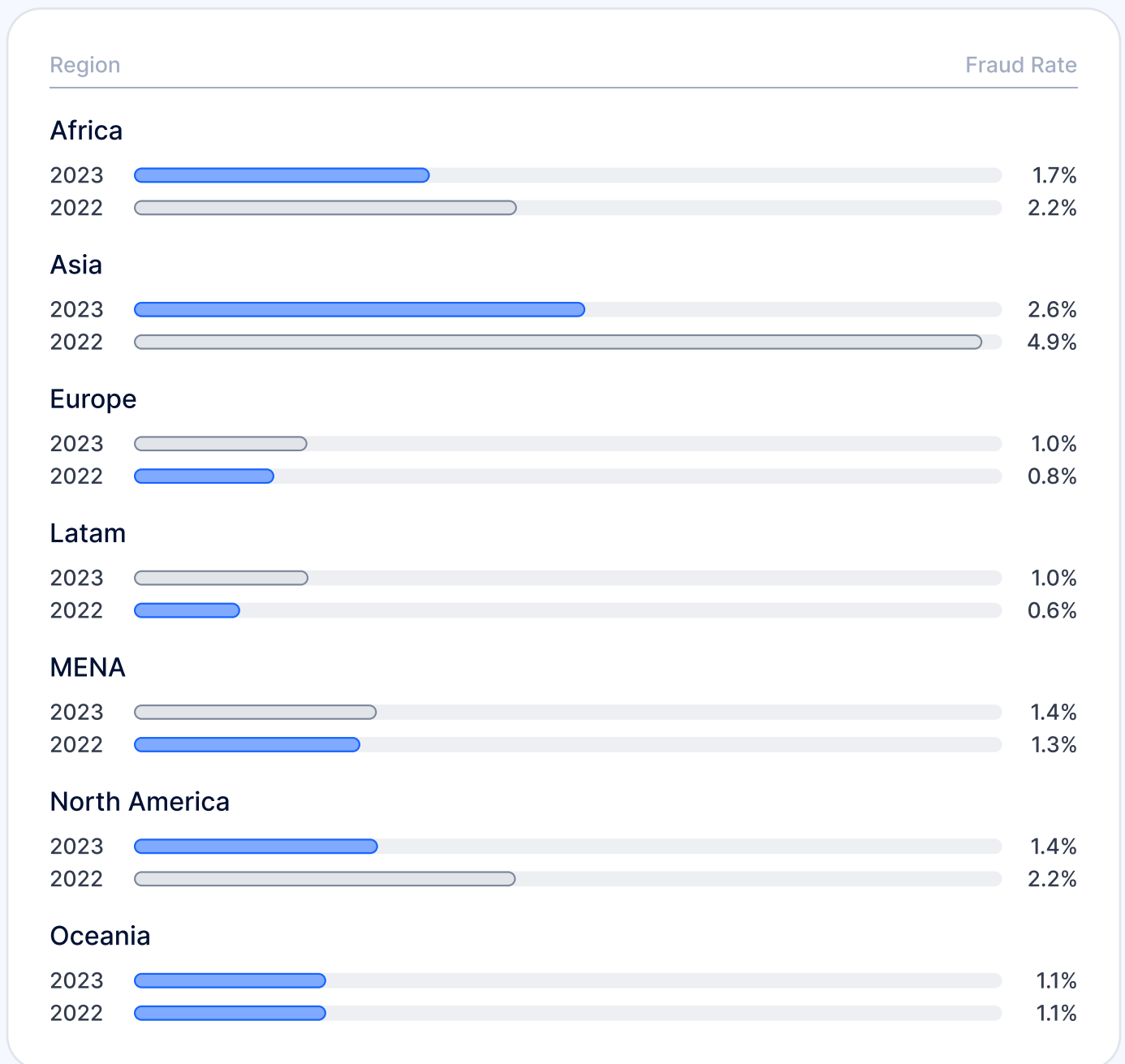
Document-based vs Non-Doc Verification results



Overall, in countries where local, Non-Doc Verification methods are available, users get a convenient and trustworthy verification process.

Fraud rates by region

In 2023, the overall number of fraud cases decreased compared to 2022. However, the situation varies by region





Fraudulent verification attempts in Asia reduced from 4.9% to 2.6% for all cases. A similar decrease has been seen in Africa and North America. On the other hand, Europe, Latam, and MENA experienced a slight increase in fraud levels.

Meanwhile, our survey participants have observed a rise in fraud-related losses. The paradox here is that, although the number of fraud incidents seems to have decreased, the level of sophistication and the resulting financial and reputational damages of fraud has actually increased.

Legacy KYC providers are unable to effectively identify advancing fraud methods, so it is evident that robust and advanced anti-fraud solutions are required.

To effectively combat advanced fraud, it is crucial for modern anti-fraud solutions to leverage AI technology for detection. AI helps in various scenarios, such as identifying imperceptible artifacts in deepfakes, searching for document templates through similarity analysis, automatically rejecting invalid applications (e.g., receipts instead of documents), and more.


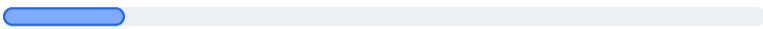
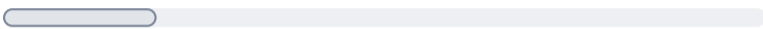

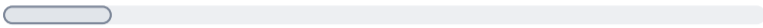
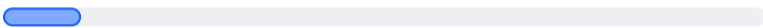

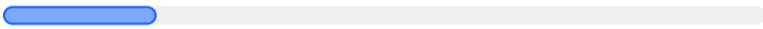
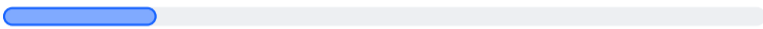

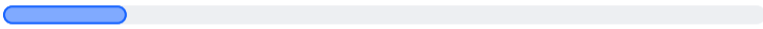
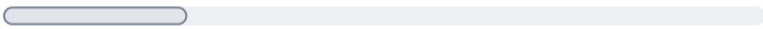

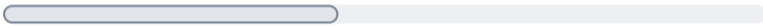
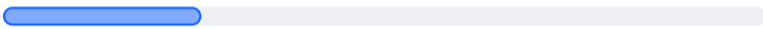

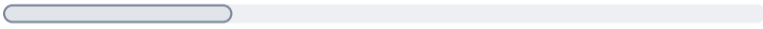
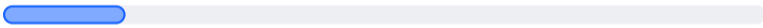

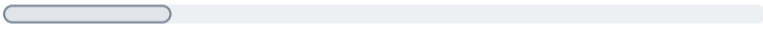
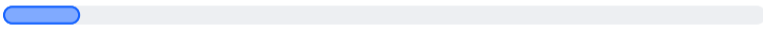

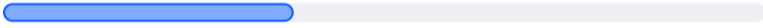


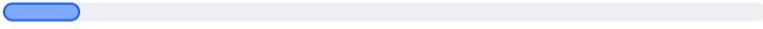
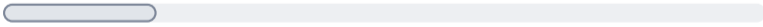

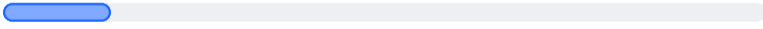
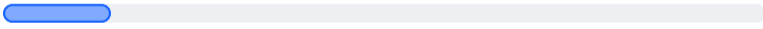

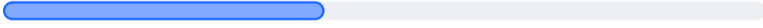


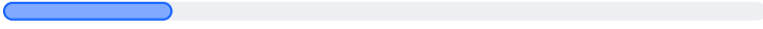
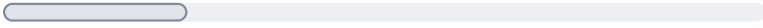

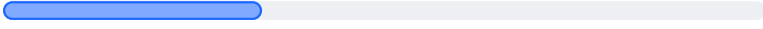

Fraud rates by countries



In 2023, Israel, Brazil, Mexico, and Hong Kong experienced an increase in fraud, though Asian Region showed promising progress with an almost two-fold decrease in fraud cases. Canada and South Africa witnessed no major changes.

Notable decreases were observed in the United States, UAE, Nigeria, and Singapore. The UK, Germany, and Australia experienced slight decreases in the number of fraud incidents. This can be attributed to greater awareness of fraud among businesses.

Fraud Rates by country

Region			% YoY Change
 Australia	2023		0.8%
	2022		1.0%
			0.2% decrease
 Brazil	2023		0.7%
	2022		0.5%
			0.2% increase
 Canada	2023		1.0%
	2022		1.0%
			0% No change
 Germany	2023		0.8%
	2022		1.2%
			0.4% decrease
 Hong Kong	2023		2.2%
	2022		1.3%
			0.9% increase
 Israel	2023		1.4%
	2022		0.8%
			0.6% increase
 Mexico	2023		1.1%
	2022		0.5%
			0.6% increase
 Nigeria	2023		2.5%
	2022		1.9%
			0.6% decrease
 Singapore	2023		0.5%
	2022		1.0%
			0.5% decrease
 South Africa	2023		0.7%
	2022		0.7%
			0% No change
 UAE	2023		2.1%
	2022		2.9%
			0.8% decrease
 UK	2023		1.1%
	2022		1.2%
			0.1% decrease
 US	2023		1.7%
	2022		2.5%
			0.8% decrease

Most popular fraud types in crypto



In the crypto industry, the primary forms of fraud continue to be traditional **document fraud**, which has been joined by the growing trend of deepfakes.

Another important problem is fraud occurring throughout the whole user lifecycle. Genuine users may pass the verification process initially, but later engage in fraudulent activities. Additionally, there is the risk of a real user passing KYC on behalf of a fraudster for monetary gain.

- i To address this challenge, companies need to implement ongoing measures like transaction monitoring and other customer lifecycle checks.



Andrew Sever

Co-founder and CEO of Sumsu



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.

Fraud types at the onboarding stage

In 2022

36% of fraud cases involved printed documents, followed by 16% where genuine IDs were altered, while 10% were entirely forged ID documents.

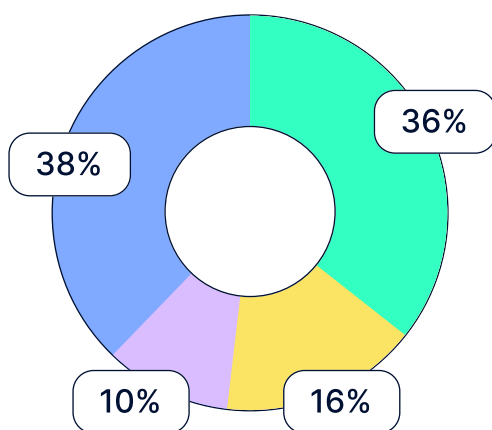
By 2023

there were notable shifts in the landscape. 53% of fraud cases involved printed documents, 6% resulted from edited real IDs, while 20% involved completely forged documents.

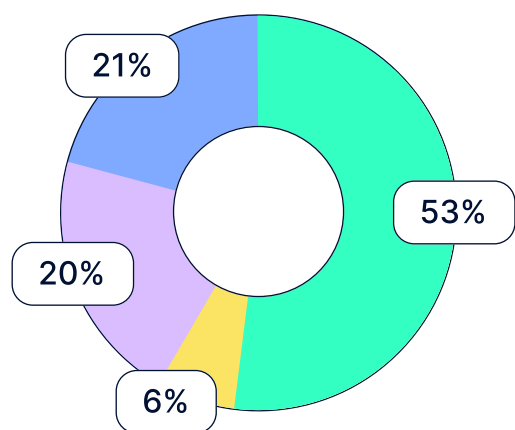
- i** The increase in completely forged ID documents shows that fraudsters are becoming more skilled and experienced.

Document fraud cases

2022



2023



● Printed docs
 ● Altered IDs
 ● Entirely forged
 ● Other

Deepfake fraud

The advancement of AI and ease of access to face swap tools have spurred the adoption of deepfake creation among fraudsters. This leads one fraudster controlling multiple deepfake accounts for deceptive purposes.

- i** Almost 10% of deepfake fraud comes from Spain, 8% from the UK, 8% from Japan and 3% from the US.

A significant threat is posed to the crypto industry. In 2023, the prevalence of deepfakes surged by 128.15% compared to 2022, more than doubling in frequency.



Pavel Goldman-Kalaydin

Head of AI/ML at Sumsu



All businesses operating digitally and performing remote verification are vulnerable to deepfake fraud. However, fintech, cryptocurrency, and gambling platforms are especially at risk.

Deepfake technology now extends to traditional document fraud. Instead of relying solely on stolen documents and pre-recorded videos, fraudsters can create fake images from scratch.

Forced verification

When someone goes through verification against their will on behalf of a fraudster, this is known as “forced verification.” In such cases, it is possible to discern that the victim is acting against their will by analyzing the photos or Liveness footage taken during verification.

Forced verification is a growing trend worldwide. According to our internal statistics, forced verification grew from 0.5% to 0.7% of all fraud cases in North America in 2022. In Q1 2023, that figure rose to 1.1%. Meanwhile, in Germany, forced verification made up 5% of all fraud in Q1 2023, compared to 0.3% in all of 2022.



Pavel Goldman-Kalaydin

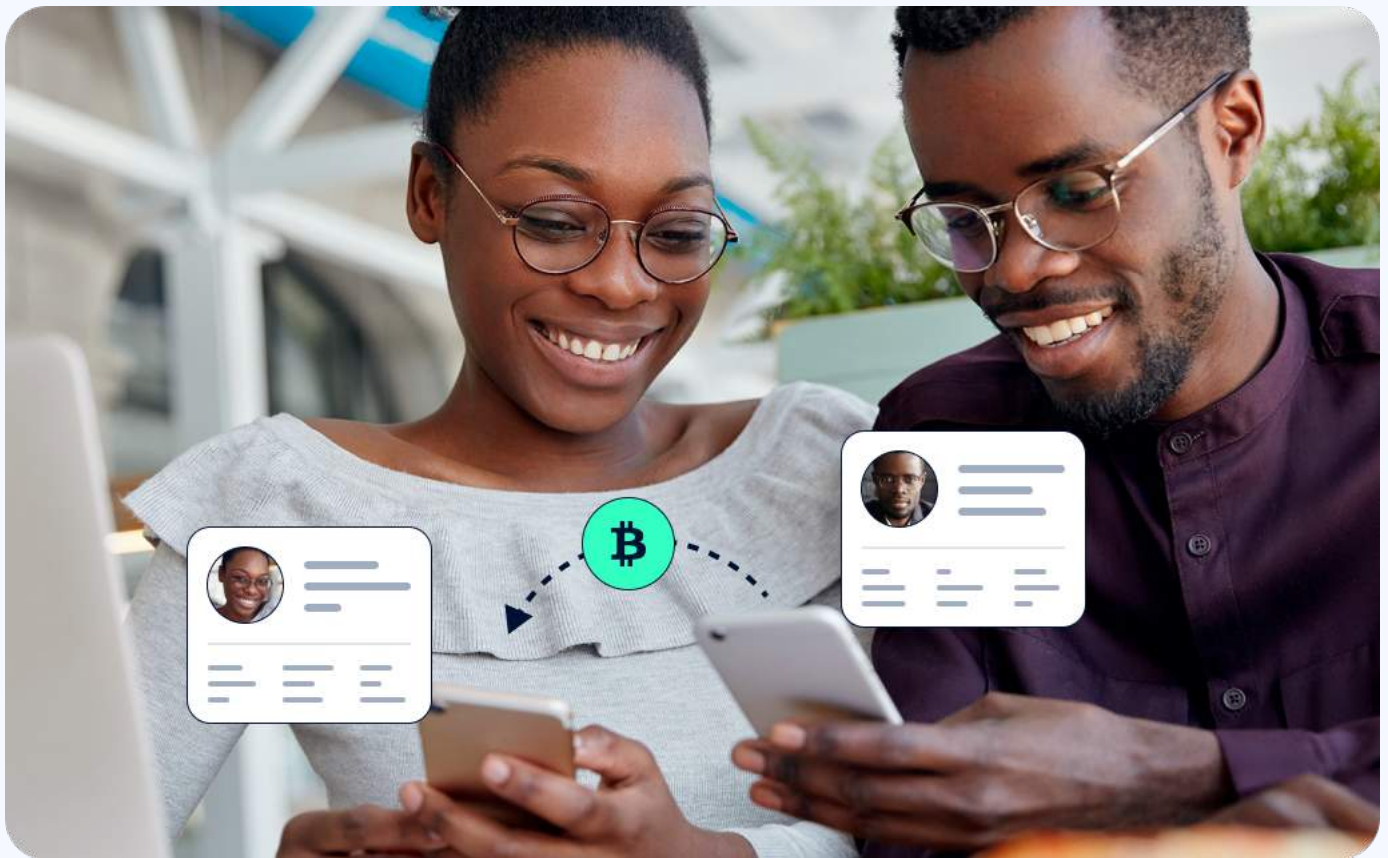
Head of AI/ML at Sumsu



It is alarming that the proportion of forced verification is growing. Likewise, sometimes the person being verified is obviously unconscious. They may be sleeping, not feeling well, or under the influence of substances. This means that they are not actively and consensually participating in the KYC process. This may lead to crime and financial fraud if not detected and stopped in time.

Forced verification can be detected with machine learning models trained in a certain way.

Regulatory changes: Travel Rule expansion



The Travel Rule refers to FATF Recommendation 16, which requires virtual asset service providers (VASPs) to collect and share customer information during cryptocurrency transfers for anti-money laundering purposes.

Global implementation of the Travel Rule is rapidly approaching. The UK mandated it on September 1, 2023 and the EU is expected to enforce it through the Regulation on Information Accompanying Transfers of Funds and Certain Crypto-Assets in 2024.

Travel Rule implementation by jurisdiction. Fall, 2023

Already implemented

Europe



Switzerland
2020



Germany
2021



Liechtenstein
2021



Estonia
2022



Gibraltar
2022



Austria
2022



Portugal
2023



UK
Sept 2023

Other jurisdictions



USA
2019



Bahamas
2020



Singapore
2020



Israel
2021



Philippines
2021



Venezuela
2021



Indonesia
2021



Malaysia
2021



Canada
2021



South
Korea
2022



UAE
2022



Mauritius
2022



Cayman
Islands
2022



British
Virgin
Islands
2022



Japan
2023



Hong Kong
June 2023

Coming soon



Lithuania
Jan 2025



EU from
30 December 2024



Su Carpenter

Director of Operations CryptoUK



"I think the biggest challenges organisations are facing this year are around the lack of clear direction and guidance being made available in relation to Travel Rule expectations. We know firms are looking at the operational readiness of complying with this guidance, but the requirements on organisations in relation to the sunrise issue and cross jurisdiction verification of transactions where there are inconsistencies in travel rule application are still a major area of concern."

To make compliance for crypto companies easier, Sumsub developed an automated Travel Rule solution in 2023.



Connect to over 500 VASPs in the Sumsub client ecosystem and enjoy free Travel Rule transfers for a whole 6 months! This offer is valid until the end of 2023

[Connect Now →](#)

Sumsub is trusted by:



Report summary

This study has derived several significant conclusions.

1 Fraud cases have decreased, but fraudsters have become more professional

Despite the overall decrease in fraud cases, fraudsters are becoming more sophisticated, making it harder to spot them due to the use of more advanced technology, including AI. Additionally, despite efforts to combat fraud, fraud-related losses are still increasing. This stresses the need for ongoing improvement in user verification.

2 The emergence of AI tools leads to new threats, such as deepfakes

AI technologies enable the creation of convincing deepfakes that can be used by fraudsters to impersonate individuals during identity verification processes. To combat this, verification systems may need to incorporate advanced AI and machine learning techniques.

3 The shift from document-based to Non-Doc Verification solutions is underway

Traditional identity verification relies on easily forged documents like passports or driver's licenses. Non-Doc solutions verify users via government databases, in some cases using digital identities and biometrics. This transition increases convenience and reduces the risk of document-based fraud in the countries where Non-Doc is allowed by regulations.

4 Compliance measures have become increasingly widespread with the global implementation of the Travel Rule

More jurisdictions are adopting measures to comply with crypto Travel Rule regulations. However, there is still a lack of universal standards from country to country.

5 Legacy verification solutions are no longer sufficient in the face of increasingly advanced fraud threats

Crypto clients are seeking comprehensive verification solutions that cover all their needs at once, including advanced fraud protection and risk assessment across the whole customer lifecycle.

How Sumsub can help

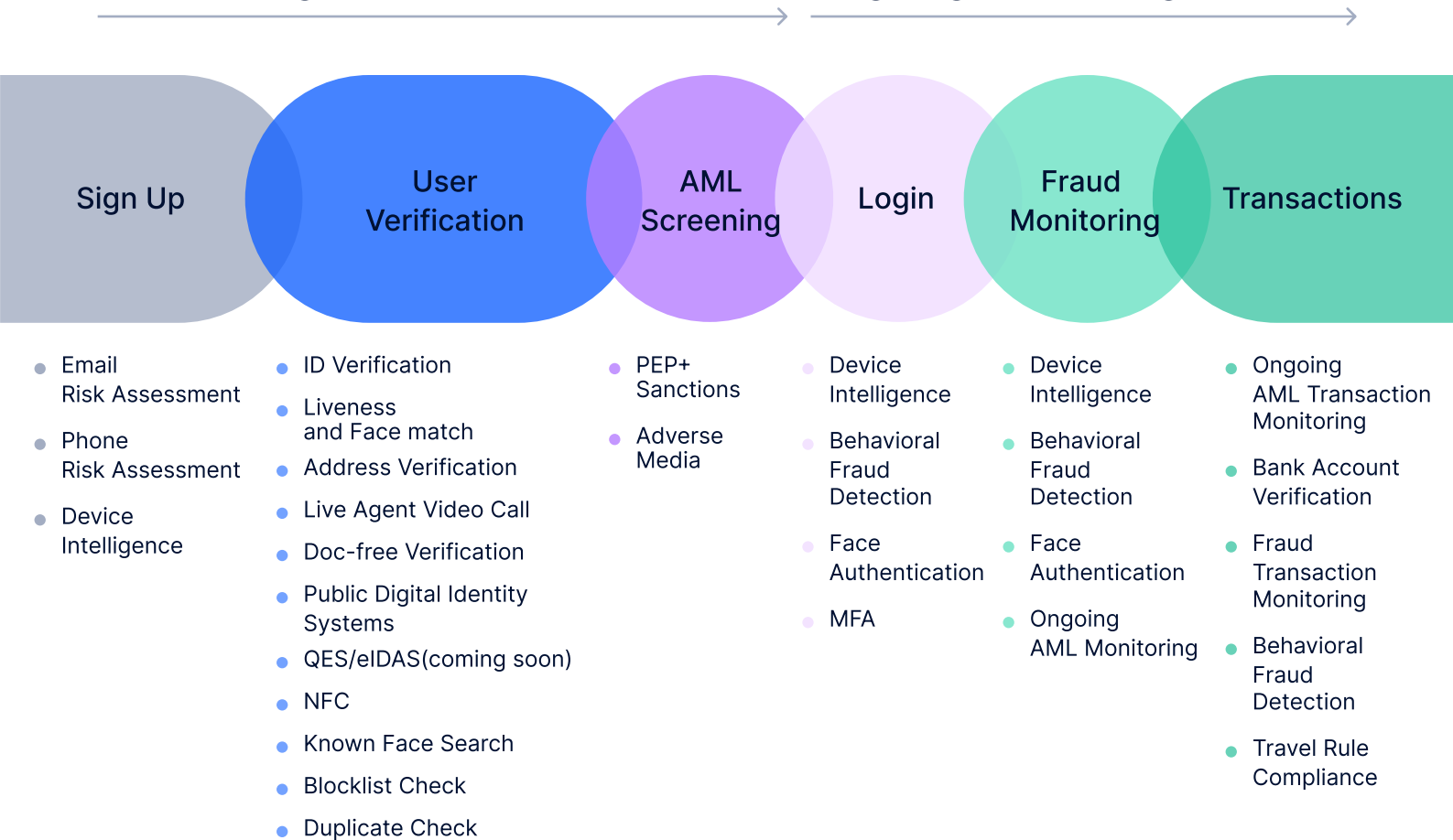
One verification platform to secure the whole user journey

Sumsub covers the whole user journey for crypto companies, 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.

Sumsub’s in-house team of compliance experts assists crypto companies in navigating complex regulatory requirements, including the Travel Rule, and successfully entering new markets.

Onboarding Orchestration

Ongoing Monitoring



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

[Get a free demo](#) →

