Sumsub Identity Fraud Study (2021)



sumsub

In this study

3 About Sumsub

4 About this study

6 Key takeaways

7 Fraud trends around the globe

11 Fraud by industry

15 How fraudsters bypass verification

20 The most forged IDs and utility bills

23 Red flags of fraud

27 Predictions for 2022

About Sumsub

We are a tech company that helps businesses verify clients with ease and stay fully compliant with shifting regulations. Our solutions are used by millions of users worldwide, and include document verification, biometric checks, video identification, payment fraud prevention, and more.

We also have several channels where our experts share insights on fraud prevention and KYC/AML compliance

Blog YouTube Facebook LinkedIn Twitter

About this study



At Sumsub, we verify millions of identities annually and stop tens of thousands of fraudsters every month. Over the past year, we've been examining how fraudsters act, what documents they forge, and how. We took a closer look at the numbers to help businesses protect themselves from existing and emerging types of fraud.

Please don't share the content of this study without giving us credit

Thank you!

© Sum and Substance Ltd (UK), 2021

Methodology

Our research took place between 2020 and 2021 and was focused on identity fraud

We defined 'identity fraud' as the use of fake or stolen identities to illegally access goods and services. Therefore, we analyzed instance of document forgery, biometric fraud (fraudsters using masks, videos, or deepfakes), and other attempts to bypass user verification.

Our data consists of:

Tens of millions

of identity checks performed by Sumsub in 2020-2021

Tens of thousands

of fraud attempts detected each month

6500+

document types from 220+ countries and territories analyzed

Our research is based solely on the data indicated above, which has been aggregated and anonymized.

The data comes from various industries including banking, crypto, trading, and gambling. All graphs and infographics are based on our data, if not stated otherwise.

Key takeaways



Fraudsters are becoming more skilled

35% of all fraud attempts are initiated by fraudsters using advanced forgery techniques and we expect this figure to rise in the future.

Fraud can happen at any stage of the verification process

Most often it happens during ID checks (65.2%). Other stages with incidences of fraud include biometric checks (6.7%), proof of address verification (5.5%), and selfie checks (0.9%).

The most effective way to stay safe

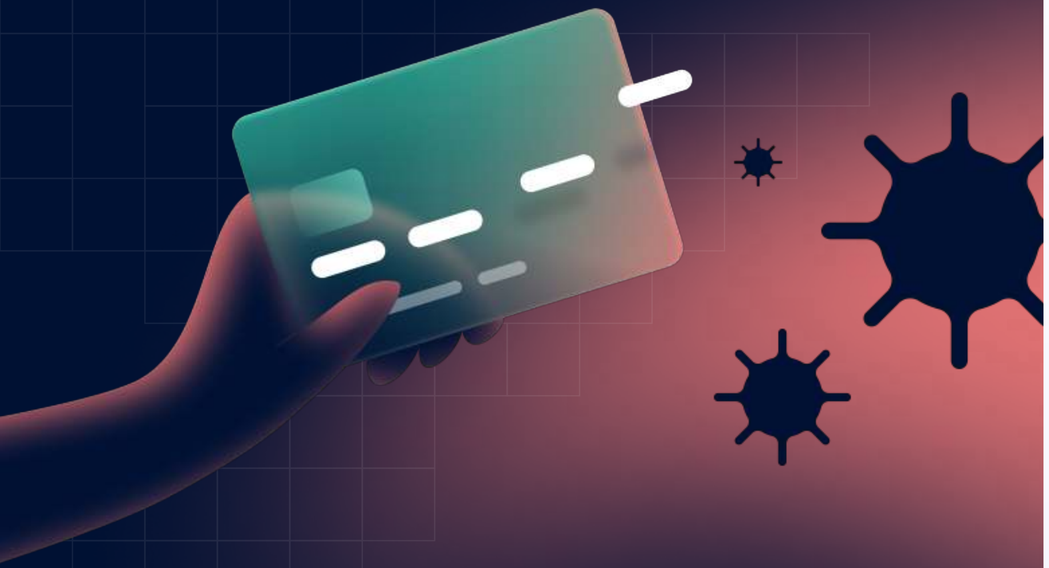
is to screen for complex fraud schemes at different onboarding stages. It's also essential to consider various red flags, including suspicious email domains and IP addresses.

Fraud trends around the globe



The worse the economic situation, the more fraud there is

Fraud rates are increasing due to COVID-19 and the growing volume of remote transactions. Meanwhile, fraud techniques are becoming even more advanced.



25% was the average increase in chargeback fraud* due to the COVID-19 pandemic, based on the 2021 Chargeback Field Report by Chargebacks911.

43% Large UK and US merchants reported an even bigger increase (43%) in illegal chargebacks.

90% of respondents stated that chargeback fraud was a concern for their business.

* Chargebacks are credit card charges that customers request over alleged disputes. This could be an honest user returning something they didn't intend to purchase, or a fraudster trying to trick the system.

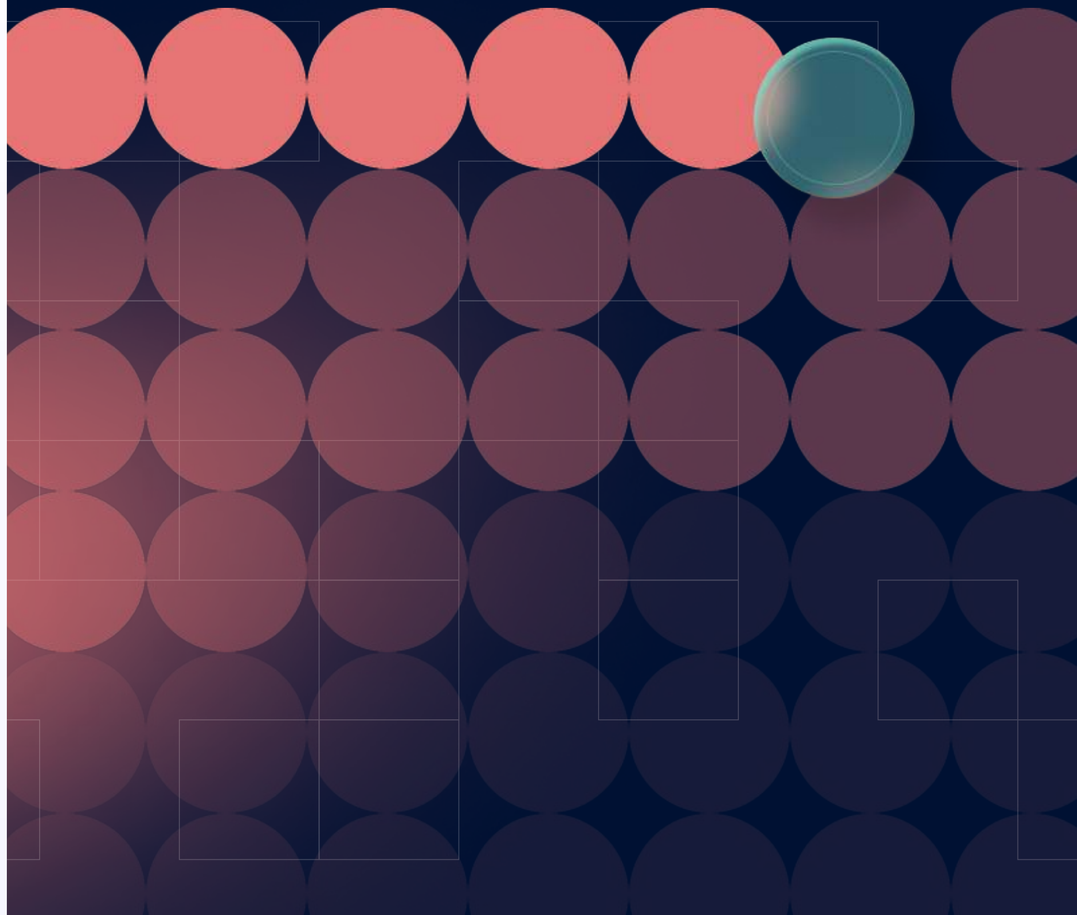
$ 56 000 000 000

was how much consumers lost to identity fraud last year in the US, according to the 2021 Identity Fraud Study by Javelin Strategy & Research. 38% of the victims closed their accounts since no resolution was made at their financial institution.

6

was the average number of fraud attempts reported per company, according to PwC's Global Economic Crime and Fraud Survey 2020. That year, PwC's respondents lost a total of $42 billion due to fraud. This figure doesn't include damages to reputation and market share, as well as possible regulatory sanctions.

Businesses and consumers are losing money



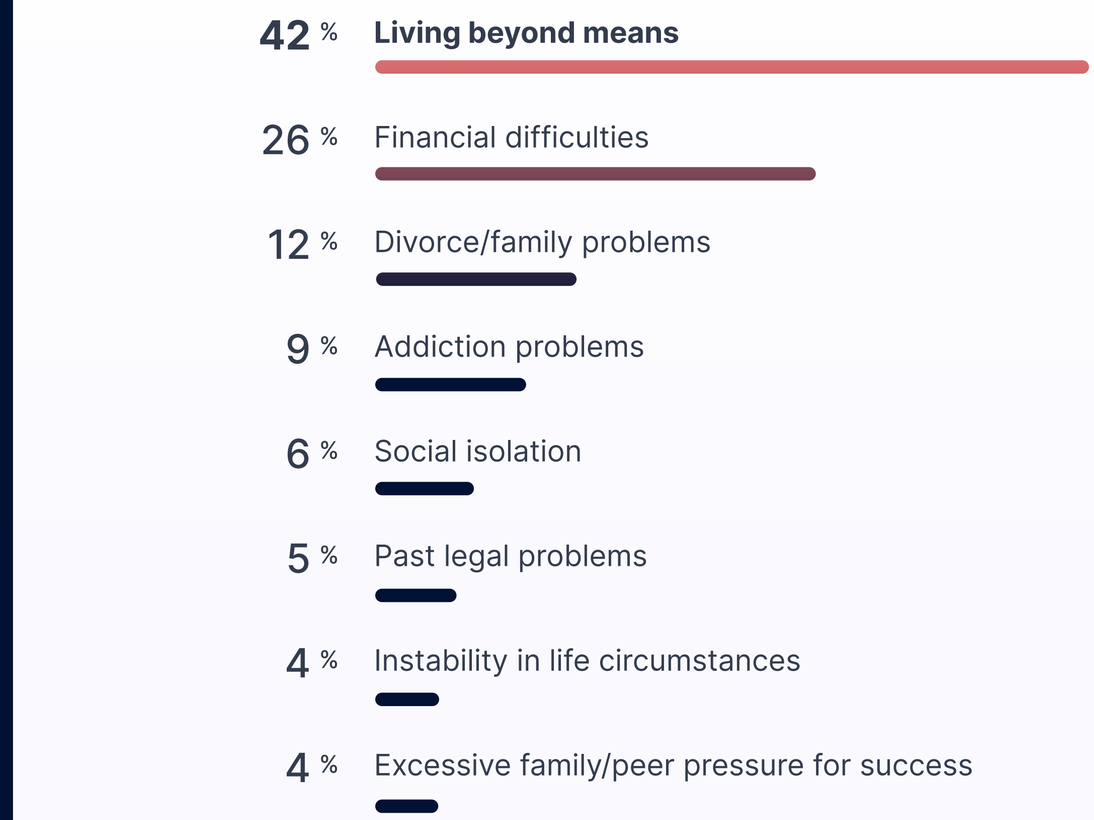
Causes of fraud

In 63% of cases, people are driven to commit fraud due to personal issues, such as addiction, financial strife, problems at home, and legal trouble.

«A fraudster living beyond his or her means is the most common red flag by a sizable margin. This has ranked as the #1 red flag in every study since 2008.»

ACFE

2020 Global Study on Occupational Fraud and Abuse, Association of Certified Fraud Examiners.



Source: 2020 Global Study on Occupational Fraud and Abuse, Association of Certified Fraud Examiners.

Fraud by industry



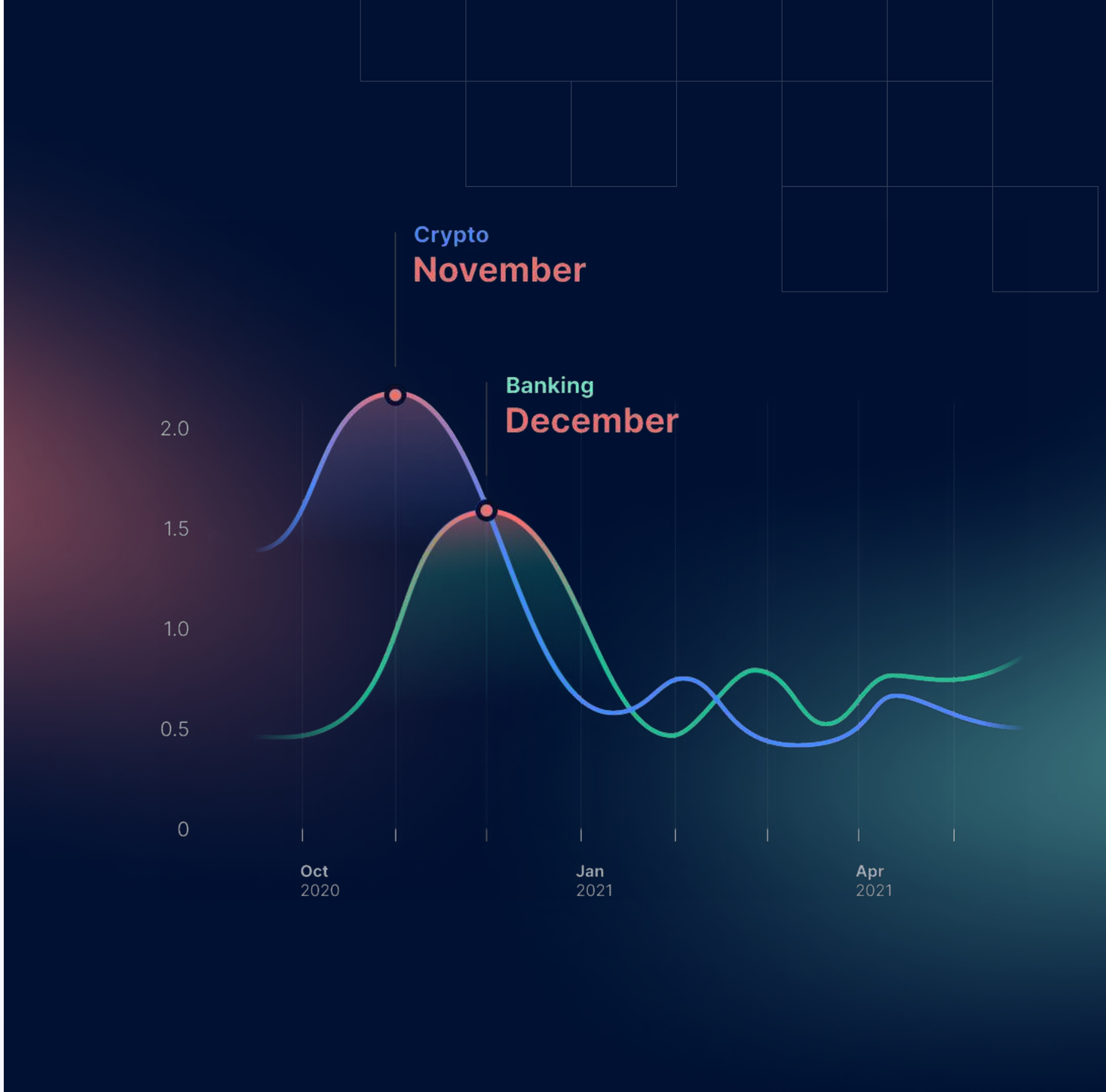
Fraud in the banking and crypto sectors

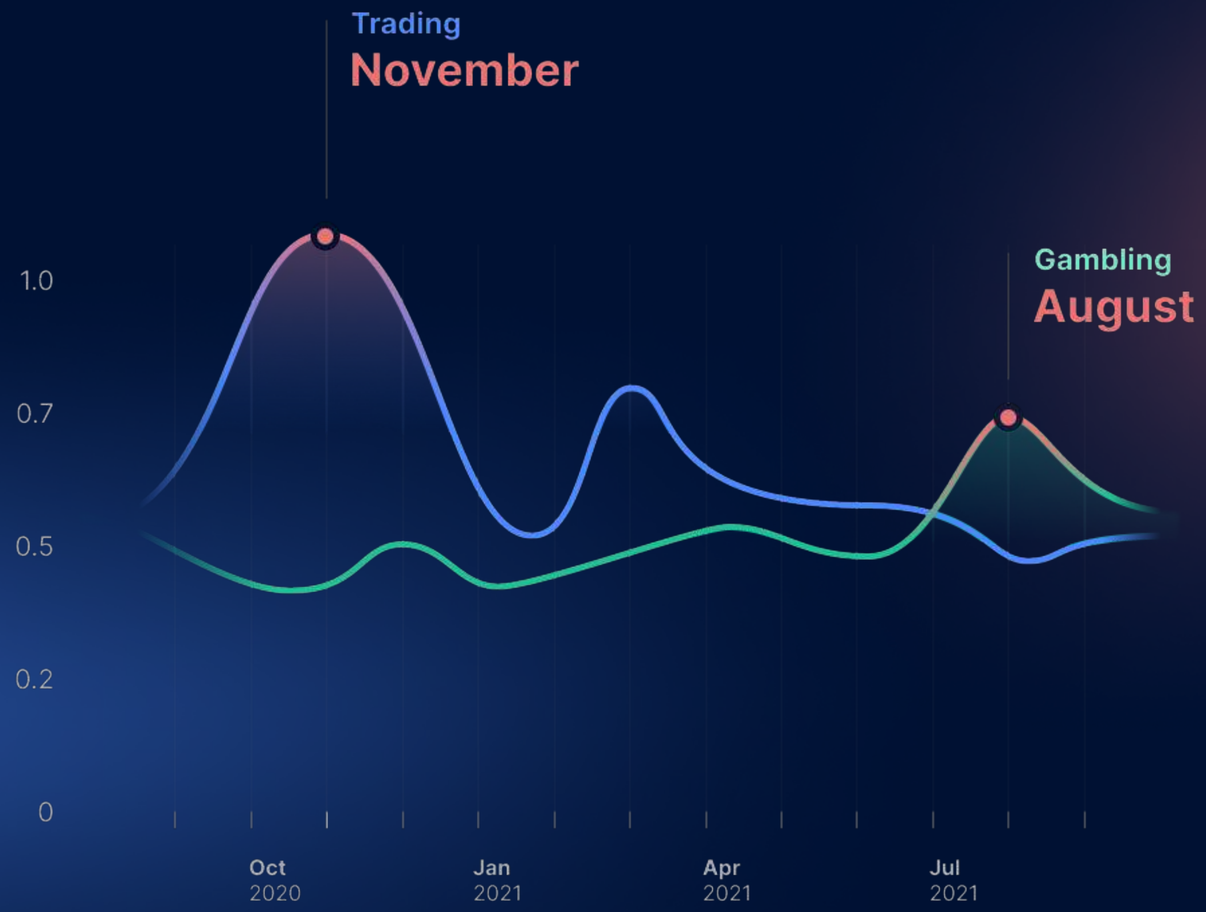
Forgery — Crypto

In the crypto sector, the fraud rate spiked in November 2020 and then gradually decreased. This could be connected to highly volatile cryptocurrency prices at the time.

Forgery — Banking

In the banking sector, our data shows that more fraud, such as illegal chargebacks, was committed during the winter holidays.





Fraud in the trading and gambling sectors

Forgery — Trading

In late 2020/early 2021, fraud in the trading sector peaked twice and then declined. There can be different reasons for the spikes, so a longer period should be analyzed.

Forgery — Gambling

The fraud level remained stable in the gambling sector. This could be explained by the lesser impact of exchange rates and inflation compared with other industries. The slight peak in August could be due to various factors, including the Tokyo Summer Olympics and the start of the European football season.

Industries with professional fraudsters

We refer to individuals who have tried to trick our verification system several times as “professional fraudsters.”

The significant number of fraudsters in the gambling sector could be due to multiple accounts created on gambling platforms for free bonuses.



7.8 %	**Gambling**
3 %	Payment
1.7 %	Crypto
1.3 %	Car sharing
1.2 %	Transportation
0.9 %	Trading
0.5 %	Banking

Professional fraudsters target gambling platforms in over 70% of cases

How fraudsters bypass verification



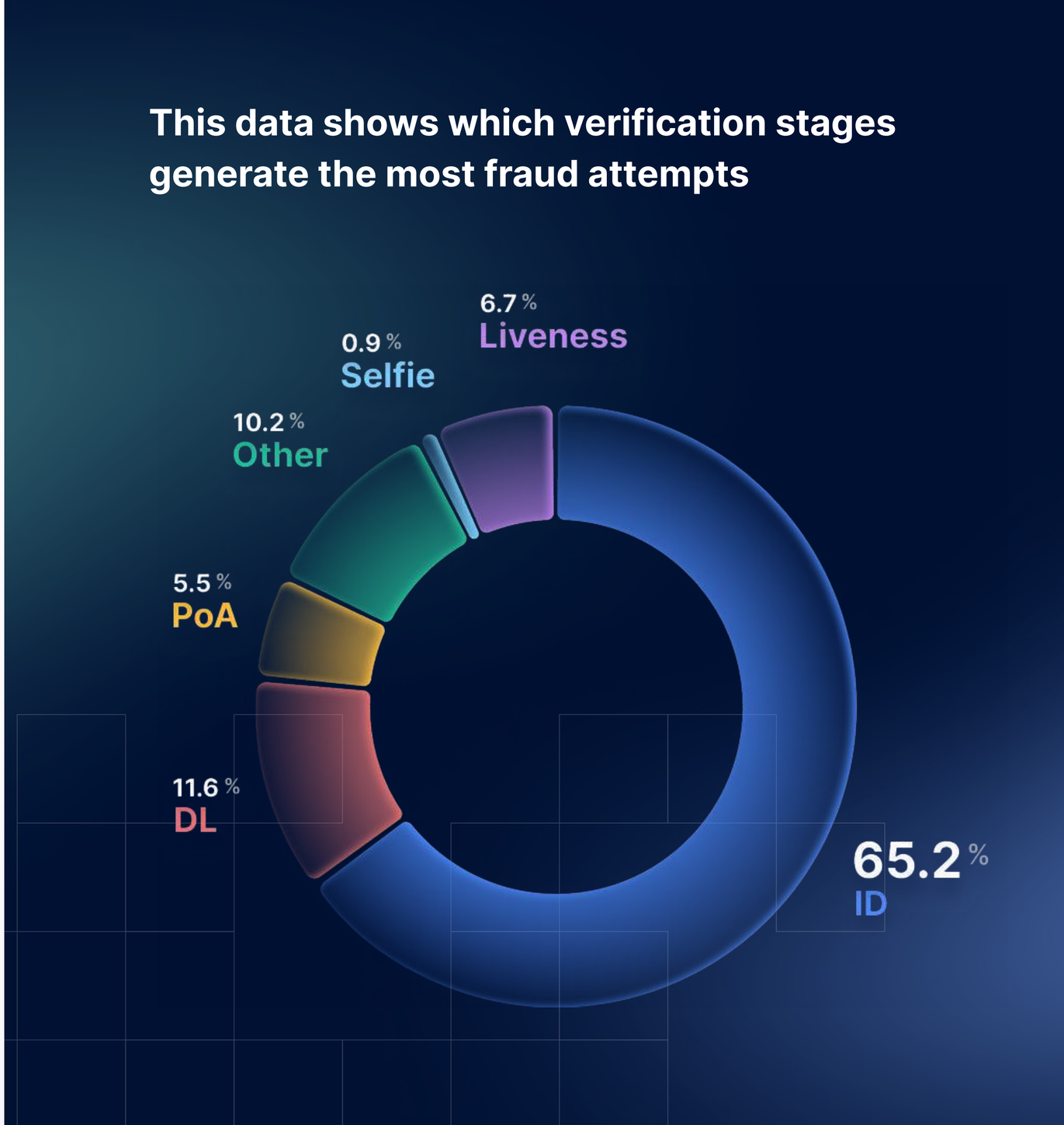
When fraudsters try to bypass verification

In about 80% of cases, fraudsters try to bypass various document verification checks (ID, DL, and PoA). 65% of cases occur during the ID check, followed by driving license verification* (11.6%) and proof of address verification (5.5%).

In about 8% of cases, fraudsters target biometric checks and selfie checks, which seek to ensure that the true document holder is present during verification.

* Driving licenses can be used either as identity verification documents or as proof that a person can legally operate a vehicle.

This data shows which verification stages generate the most fraud attempts



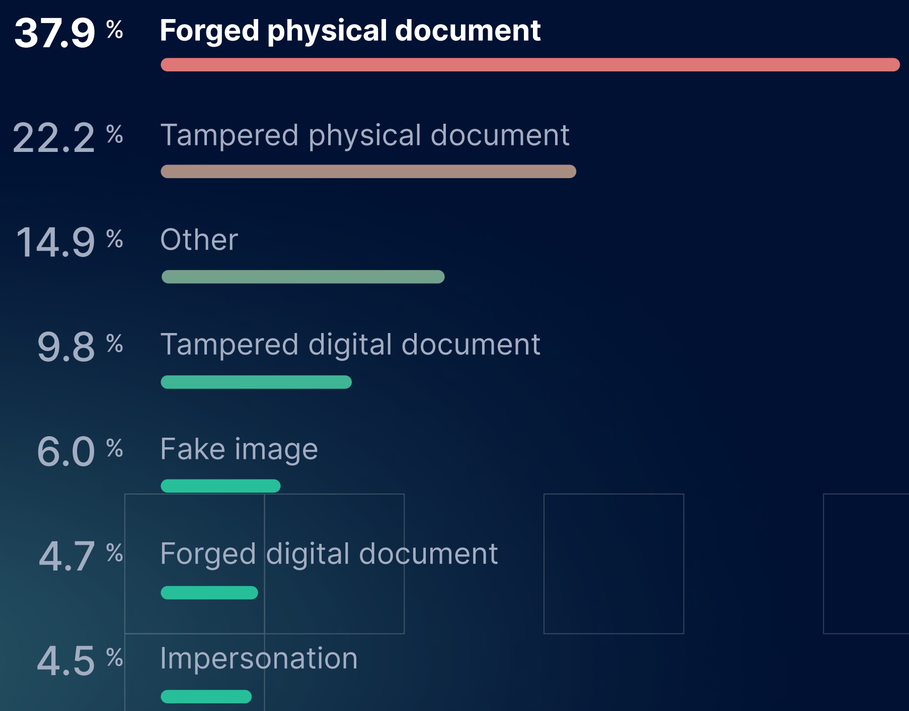
How fraudsters forge documents



of fraudsters use physical fakes to trick the verification system

In a third of cases, fraudsters recreate a whole new document. In 22% of cases, they tamper with a valid document. For instance, fraudsters can create a fake document using a graphic editor, print it out, and use it during onboarding.

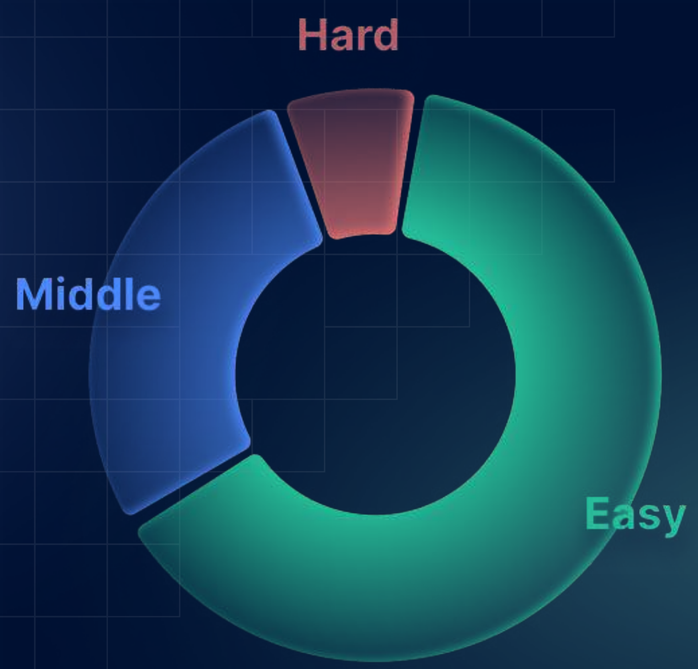
Digital forgeries occur when fraudsters submit digitally-edited pictures or PDF-files of documents. These are less common than physical fakes, accounting for just 14.5% of all forgeries.



Difficulty levels of forgery

35%

of forgeries belong to the ‘middle’ and ‘hard’ levels of difficulty. This means that a third of all fraud attempts are initiated by fraudsters using advanced forgery techniques.



65.3%

Easy

These forgeries can be detected by the human eye, as key document elements (fonts, colors, etc.) are clearly wrong.

27.4%

Middle

These are errors that are less obvious to the human eye. The overall look of the document could be right, but the colors of some security features could seem off.

7.3%

Hard

These cases require superior knowledge of document manufacturing and security features. Such forgeries can be noticed only by verification experts and advanced verification systems.

Case study



1

A fraudster buys photos of a valid ID along with a selfie of the true document holder on the darknet.

2

The fraudster uses the photo of the ID during the onboarding stage to get access to a service.

3

The verification system cannot recognize any signs of forgery, since the document is technically valid.

4

The fraudster gets to a facial biometric check. They try to bypass it by presenting the selfie of the true document holder.

5

The facial recognition system scans the presented image, checking its depth, eye reflections, skin texture, and more.

6

The check determines that there isn't a real person in front of the screen, but just an image. The fraudster is denied access.

The most forged IDs and utility bills



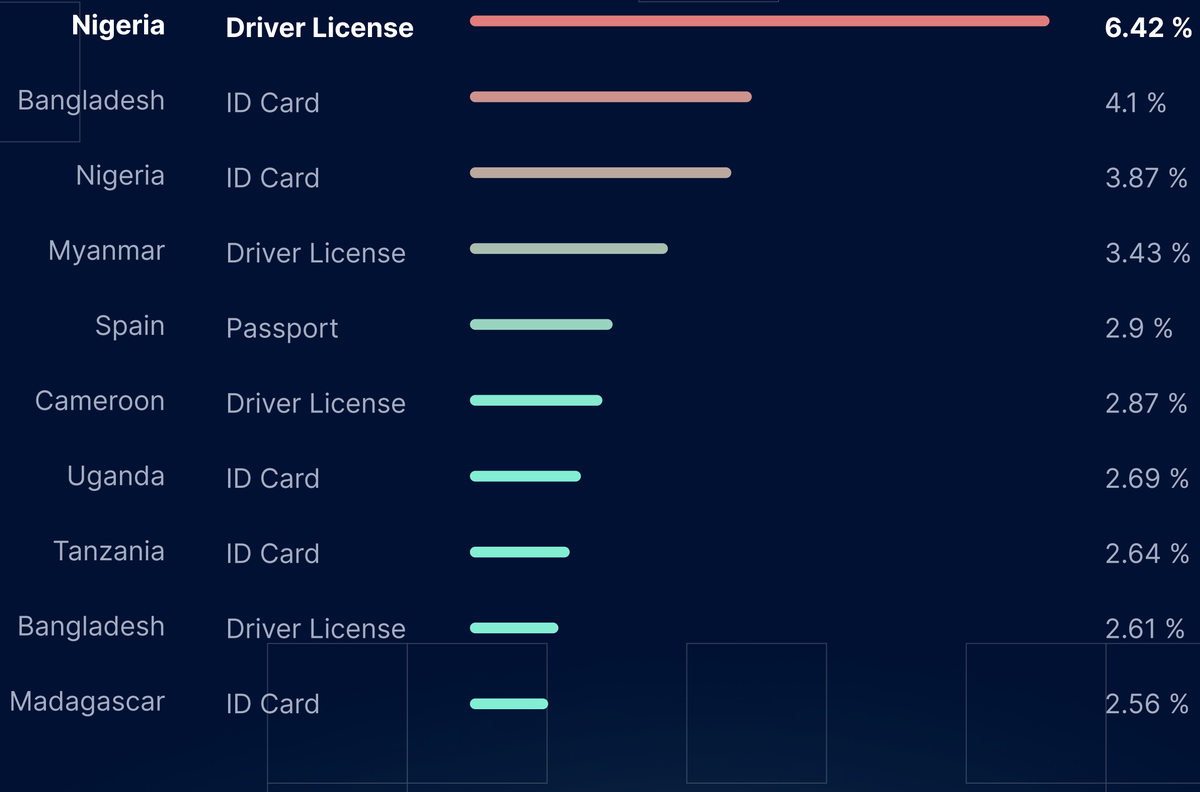
10 most forged ID documents

Here are three factors that contribute to the prevalence of forgery in certain countries:

1. Low document security, including absence of security features like watermarks, holograms, and stamps;

2. The presence of legal loopholes allowing fraudsters to create digital forgeries without facing criminal liability;

3. Low privacy-awareness among citizens leading them to unknowingly upload their documents to suspicious websites.





6.4% of all forged documents are Nigerian driver's licenses, while 3.8% are Nigerian ID cards

10 most forged utility bills

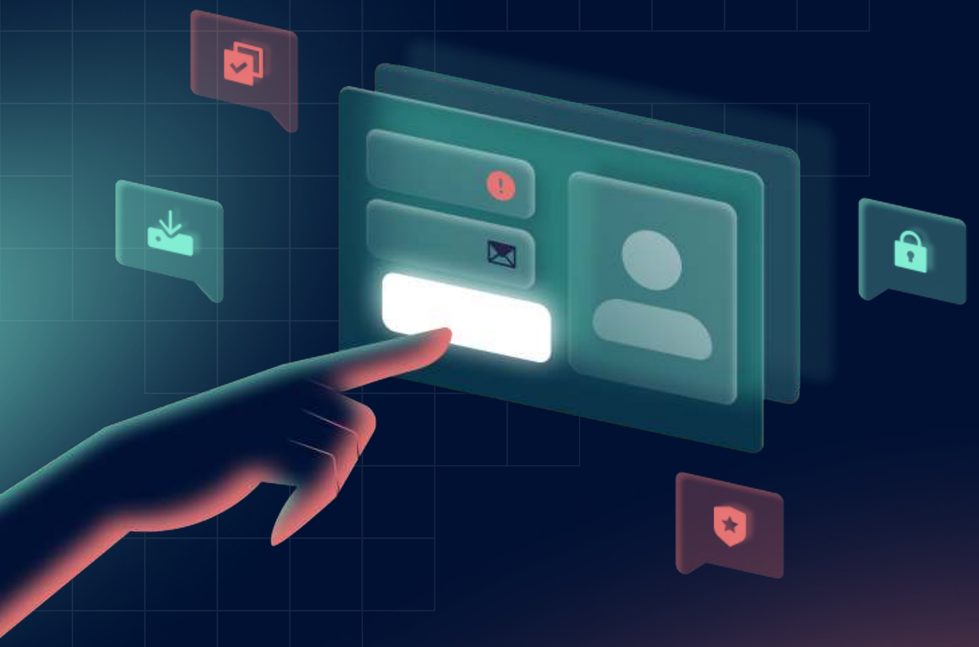
Utility bills are used to prove an applicant’s address. These documents are generally easier to forge than ID documents since they usually have no security features.



Red flags of fraud



Here are are some key fraud indicators that businesses should look out for when onboarding new users*



- **Duplicate profiles;**
- **User uploads different ID documents;**
- **User is a Politically Exposed Person (PEP) or is featured in adverse media;**
- **Data on documents is inconsistent and/or the user's face doesn't match the photo in their documents;**
- **Onboarding request comes from a high-risk jurisdiction (see the FATF's list of jurisdictions under increased monitoring);**
- **Suspicious, undetectable, or non-matching IP location;**
- **Suspicious email domains.**

* Please note that the presence of a single red flag may not be a sufficient basis for denying a user access.

Suspicious email domains and IP addresses

Here are the top email domains and IP locations that fraudsters use to register with platforms. We suggest adding these email domains and locations to your list of red flags and paying extra attention to customers that use them.

Top 10 email domains with fraud attempts

39.23 %	assism.net	8.65 %	emailn.de
23.68 %	mailo.com	8.37 %	yopmail.com
23.04 %	inbox.eu	6.64 %	cox.net
20.79 %	rover.info	6.35 %	gmx.com
8.81 %	usa.com	4.77 %	att.net

Top 10 IP locations of fraudsters

4.17 %	Nigeria	2.38 %	Bangladesh
3.41 %	Tanzania	2.17 %	Albania
3.02 %	Uganda	1.95 %	Ivory Coast
2.84 %	Zimbabwe	1.42 %	Tunisia
2.56 %	Cameroon	1.41 %	Pakistan

Fraud rates by browser and operating system

In general, we don’t see a big difference between platforms and browsers when it comes to the number of fraud attempts initiated.

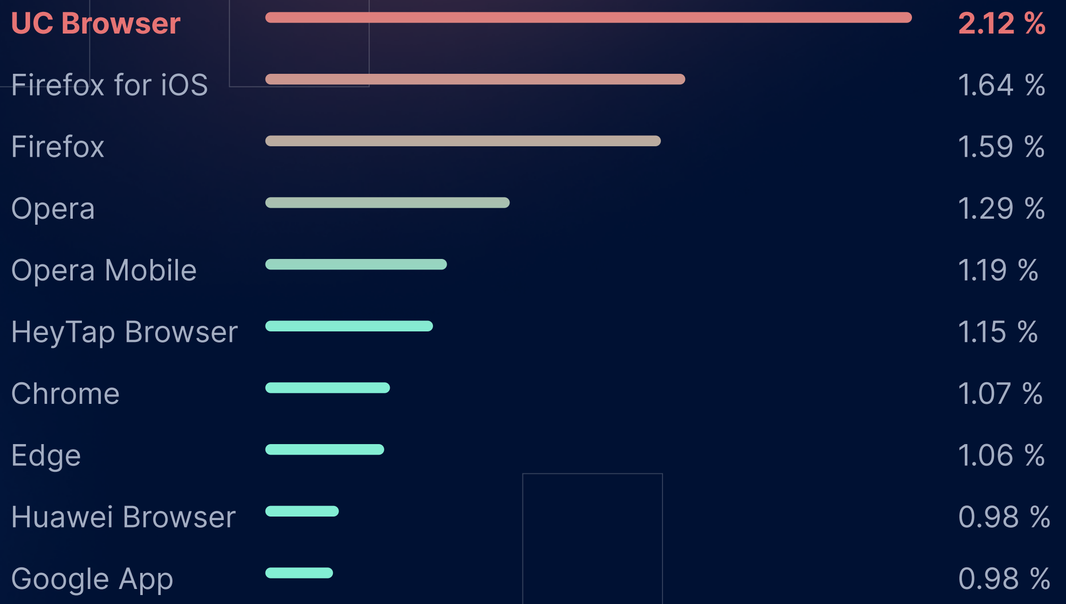
PC



Phone



Top 10 browsers with fraud attempts



Predictions for 2022



Here are our predictions for next year, based on the identity fraud trends we're currently seeing

Fraudsters will continue to exploit COVID-19

Since the pandemic started, we've seen countless cases of COVID-related fraud, including impersonation and phishing. This trend is likely to continue next year. In particular, we expect fraudsters to forge COVID passes.

Next year, forgeries are likely to become even more advanced

As businesses around the globe introduce stronger verification solutions, including biometric checks, fraudsters are developing new ways to bypass them. More specifically, we think that fraudsters will be using biometric forgeries such as deepfakes.

The number of electronic identity documents is likely to grow

In recent years, governments around the globe have introduced electronic ID documents. This trend is likely to continue. Some of these documents may have fewer security features, which makes them easier to forge. To protect against them, businesses can add additional checks to their verification flow, including facial biometrics and QR code verification.



Fraud rates aren’t going to decline. This is an eternal game of cat-and-mouse: criminals come up with new fraud techniques, and we learn to catch them.



The biggest danger is deepfakes. At present, it’s difficult for an ordinary person to make a high-quality deepfake—but soon, I'm afraid, technologies will reach the point where everyone can make a realistic deepfake on their phone in 2 seconds. We must not lose our vigilance and work ahead of fraudsters. The good news is: I expect that soon many documents will have chips that allow documents to be validated. Also, I hope that governments themselves will provide ways to validate documents.

Vyacheslav Zholudev,
Sumsub’s co-founder
and Chief Technical Officer

How Sumsub helps businesses prevent fraud

To protect businesses from fraudsters, Sumsub's verification solution has the following features built in:







Security features check

Screens features like stamps, holograms, and watermarks to ensure authenticity.

Screenshot and screen recapture check

Ensures that genuine photographs are submitted rather than screenshots.

Anti-photoshop deck

Detects signs of graphic editing on submitted documents.

How Sumsub helps businesses prevent fraud









Behavioral risk score

Employs device fingerprint analysis to track suspicious user configurations and location mismatches.

Blocklist check

Identifies fraudsters by checking them against databases of blocklisted and banned persons.

Duplicates check

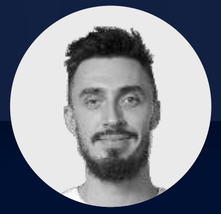
Detects when applicants try to create multiple accounts.

Facial biometrics

Conducts real-time biometric checks to ensure that the true document holder is present during verification.

Our customers say it best

"Fraud persists in the crypto industry. Price fluctuations attract not just honest investors, but fraudsters as well. This has pushed us to enhance our security measures. Sumsub has provided graphic editor detection and metadata analysis, further consolidating our protection against forgery and scams."



Andrey Ilinsky,
CPO at Mercuryo.io

"We looked at other KYC solutions, but we felt more confident in Sumsub’s fraud prevention technologies, which include liveness detection—one of the most secure verification methods now. I tried to pass Sumsub’s onboarding using false documents, but the provider detected the attempt."



Théo Rougon,
a risk manager at Bling



Want to know more about how to protect your business from fraud?

Get a free demo →