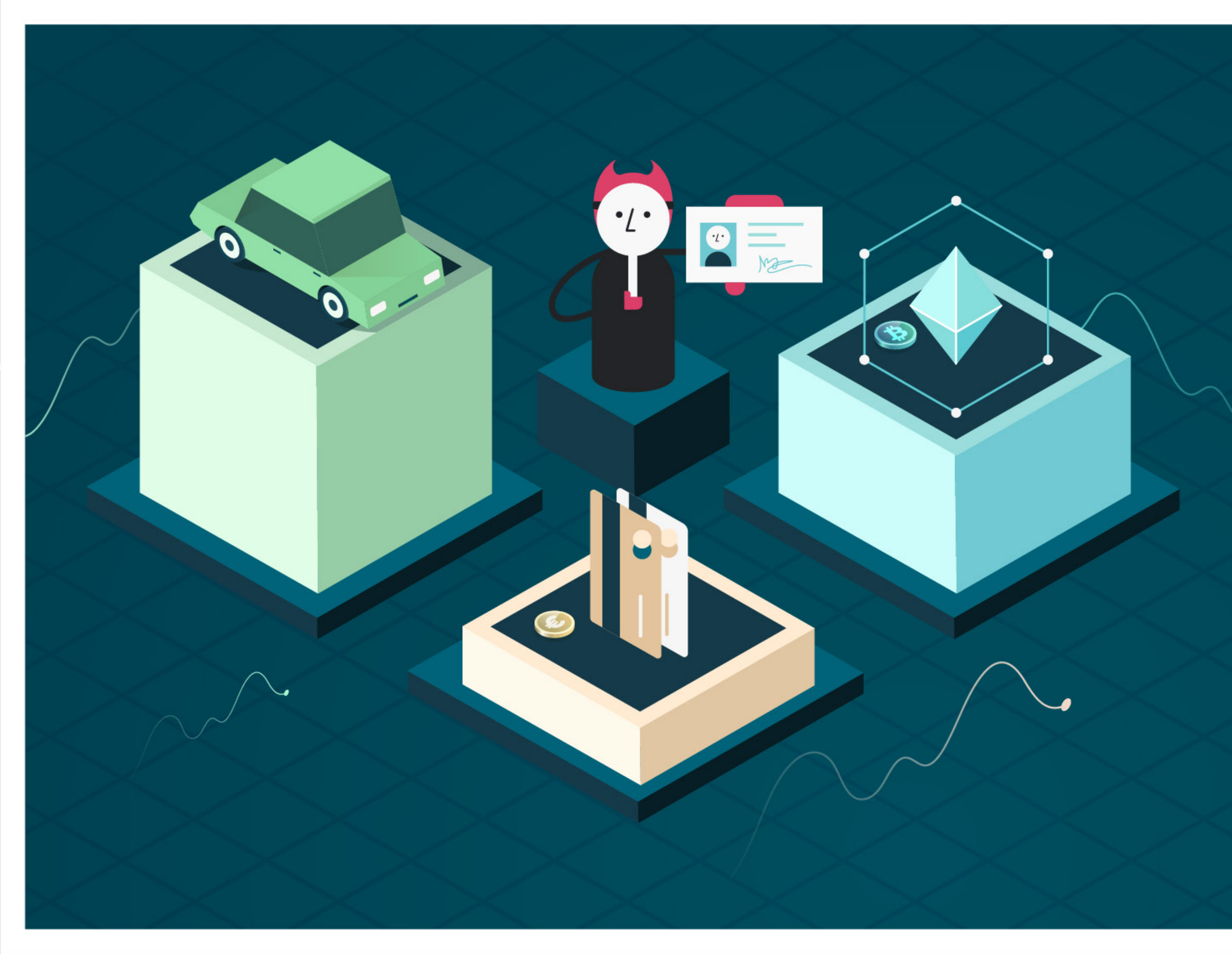
veriff

Fraud Report 2020

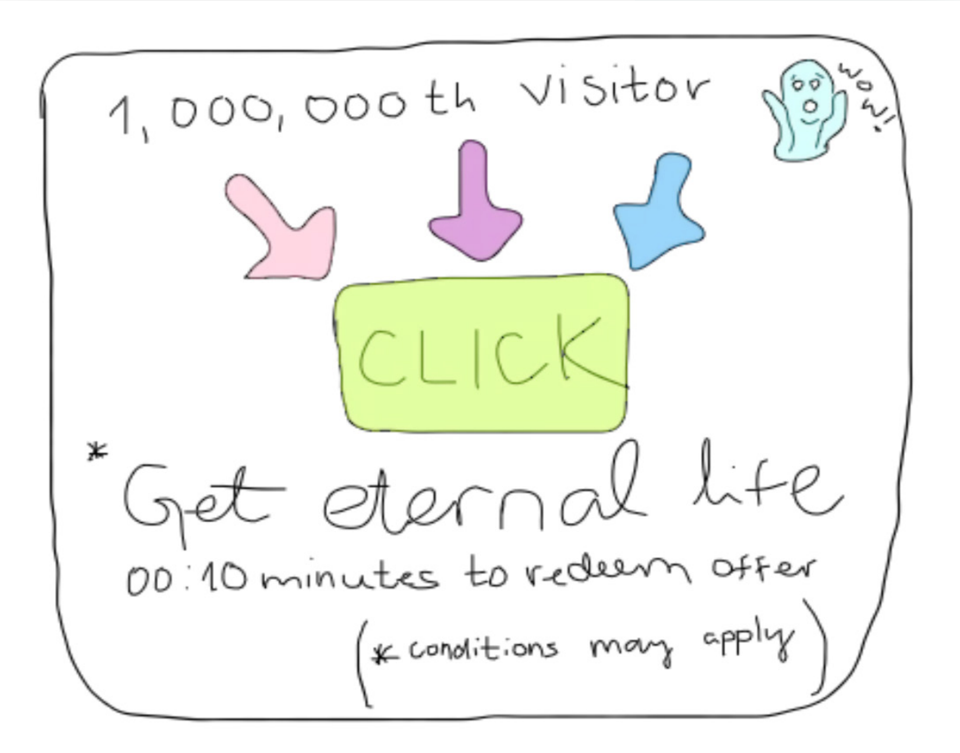


veriff

Introduction

One of the most common types of internet fraud is phishing scams. These usually lure people in with a promise of great reward upon completion of verification. Thankfully, we at Veriff use sophisticated fraud prevention tooling to detect and block fraudsters that try getting access to your verification. These fraudsters usually assure a great bounty, like receiving an immense inheritance or winning fancy prizes, but that's not always the case. As in one case, all it takes to lure people into revealing their identity is a promise of a box of 'chocolates. Veriff is here to save you from the disappointment of an undelivered box of chocolates.

Illustration by Miina Vilo

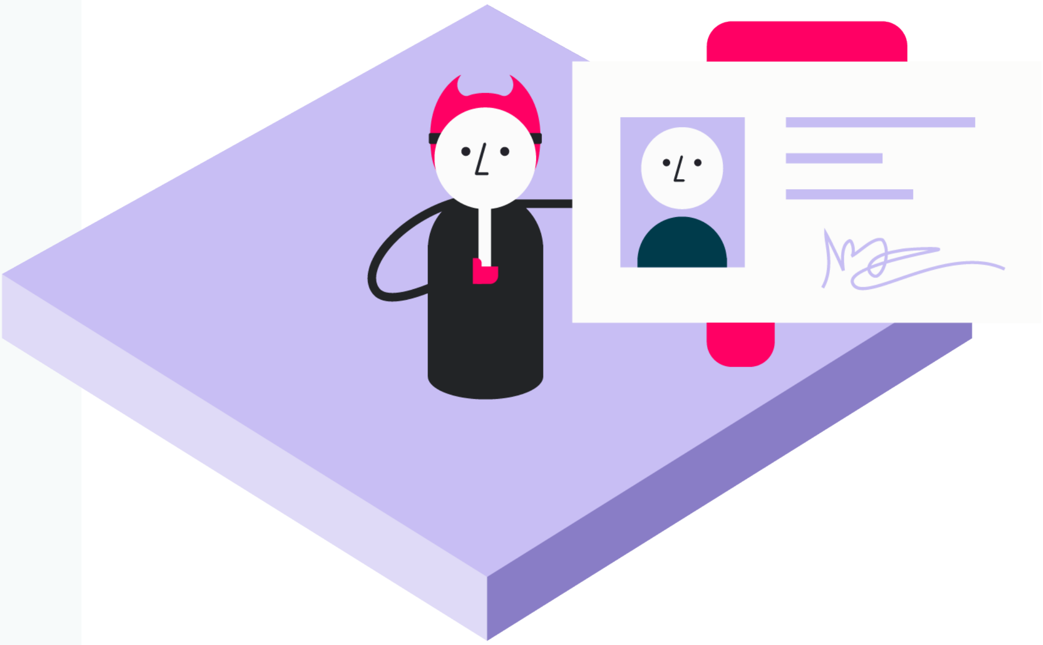


When we talk about identity fraud one might think it started occurring when the information age began and technology enabled fraudsters to commit identity theft, but that's not the case. Identity theft goes back way before the digital age, where any record of stealing personal information with the aim of committing fraud was considered an identity theft. Take for instance, election fraud during the 1800s in the US, when the paper ballot system replaced voice votes and enabled cooping.

Today perpetrators use the identity of others to violate the law by stealing money, obtaining loans and trading data in a way that their typical victim wouldn't notice the crime immediately, only realising once the major damage is already done. Criminals use various techniques to get your personal data, such as phishing, spreading malware, social engineering and other tactics you can read about in our blog.

In 2019, out of the 3.2 million identity theft and fraud reports received by Consumer Sentinel Network, 1.7 million were fraud-related, about 900,000 were other consumer complaints and about 651,000 were identity theft complaints with a reported more than $1.9 billion lost, an increase of $293 million from 2018. And according to Statista, the risk of identity theft has increased significantly since the coronavirus outbreak and is expected to increase even more in the coming months.

At Veriff, our fraud specialists analysed millions of verifications from across the globe to see what the identity verification fraud trends were in 2020. The overall fraud rate is definitely on the rise, which isn't surprising considering all the businesses that are moving online because of the pandemic. Considering the growing trend, it's crucial to be sure your customers are who they're claiming to be. This is where a digital identity verification provider like Veriff comes into its own, and here are 5 reasons why your company needs Veriff.



Key Takeaways

A global view

The United States is the leading country when it comes to fraud when compared to more than 190 countries, with a close to 10% fraud rate, followed by Vietnam (9%) and Nigeria (5%).

Pandemic-induced fraud

Due to more online activity as a result of the pandemic, there was an more than a 3 times increase in the overall fraud rate in the fintech and mobility sector. The crypto sector remained high but was more stable with no jumps.

Most common document fraud

When looking at the document types that fraudsters use the most to illegally verify an identity, Veriff saw that over half of them use an ID card (51%), followed by a driver's license (27%) and a passport (19%).

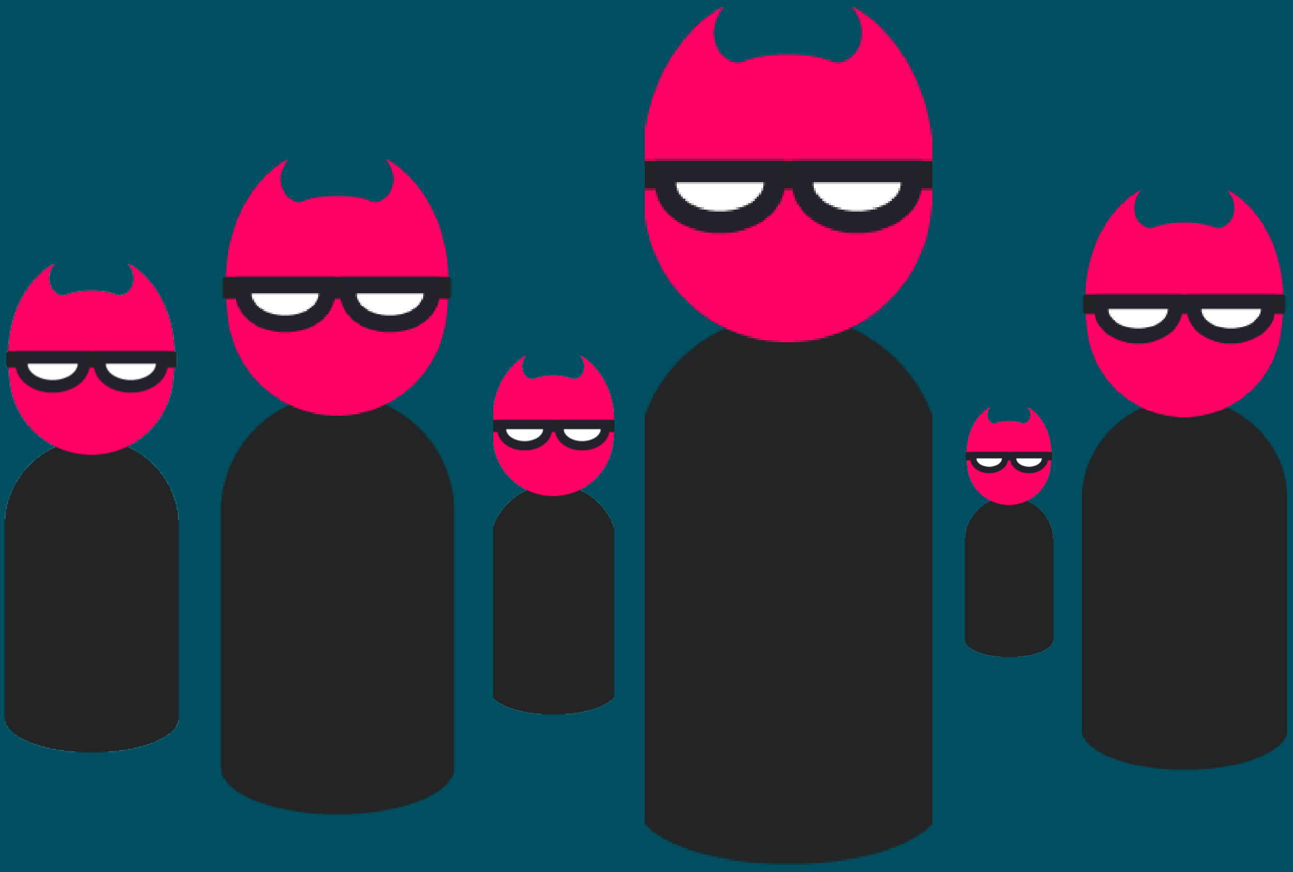
and more...

Industry differentiators

The mobility industry experienced the highest fraud rate in the second half of 2020 compared to the first half, with a 16% increase. Similarly, the fintech industry experienced a 7% increase and cryptocurrency saw a 11% increase.

Identity fraud rises

Identity fraud is the second most prevalent type of fraud in crypto (40%) after recurring fraud, and the most prevalent type of fraud in the fintech industry (70%). Comparing it to the first half of 2020, Veriff saw an 11% increase in identity fraud in the second half of the year.



What is Online Fraud?

Online fraud is the use of online services, or some malicious software with internet access, to defraud people or to otherwise take advantage of them. Some of the most common fraud types include new account fraud and account takeover fraud. In case of new account fraud "synthetic identities" are created to start using online services. These identities are either faked, stolen, modified from real data or simply bought on the dark web. In the case of account takeover criminals get access to people's accounts and start doing online transactions on their behalf.

The Rise of Deepfakes

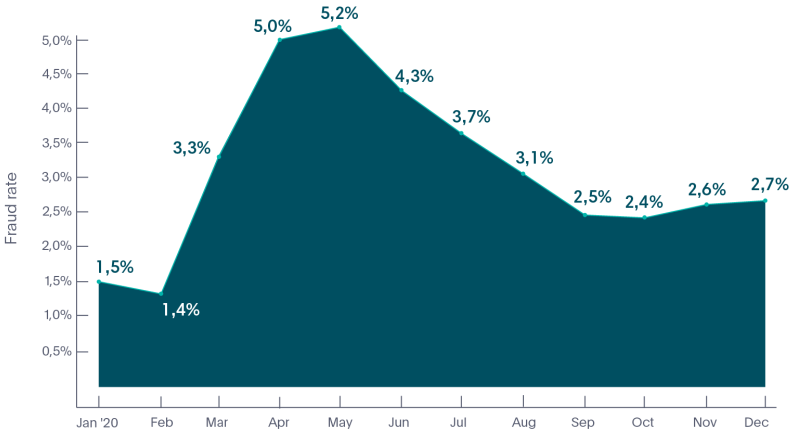
A most recent growing phenomena in online fraud is deepfakes - synthetic media whereby an image or video of a person is replaced with the likeness of someone else. Veriff encounters deepfakes on a daily basis as fraudsters are trying to beat the system to get through our flow. However, the technology we use at Veriff is much more sophisticated and does not only rely on biometrics. Instead, we combine many different data points when detecting fraud. The year 2020 witnessed an increase in online fraud, especially due to the COVID-19.

The Impact of Covid-19 on Fraud

Due to the lockdowns around the world, people started doing more things online. The pandemic caused a huge rise in the adoption of digital solutions, changing the way that many industries operate. [Arkose Labs Q4 2020 Fraud and Abuse Report] reveals that fraudsters quickly adapted to evolving changes causing the attack volume in 2020 to double compared to the second half of 2019 and a 25% attack rate increase across all transactions. Here's what we saw in Veriff in the course of the year 2020. Fintech fraud more than tripled in spring during the initial Covid outbreak, reaching over 5% as people moved their banking more online (see Graph 1).

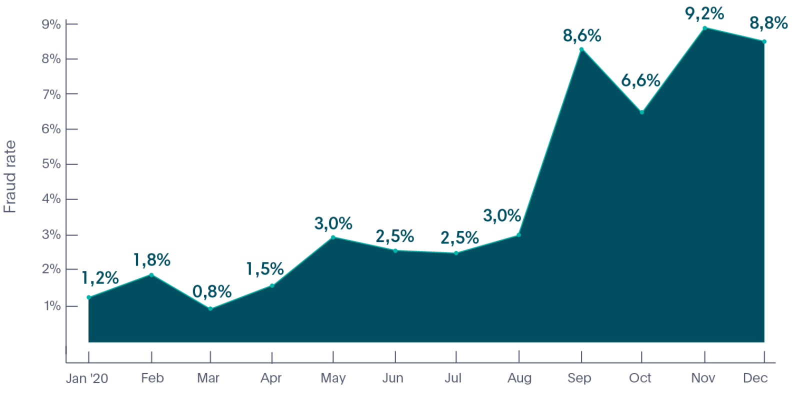
Graph 1

Fintech Fraud Rate in 2020



Graph 2

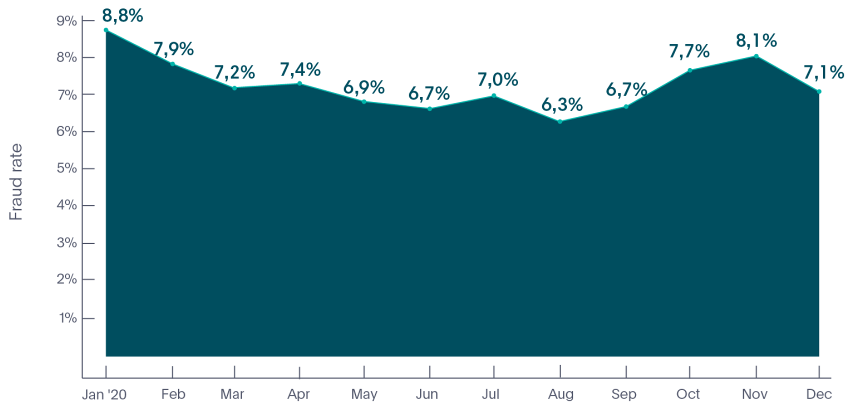
Mobility Fraud Rate in 2020



Mobility fraud showed a sharp increase starting in September as more mobility service providers went live and people started using more ride-sharing services, including scooters, mopeds and cars as an alternative to public transportation because of Covid (see Graph 2)

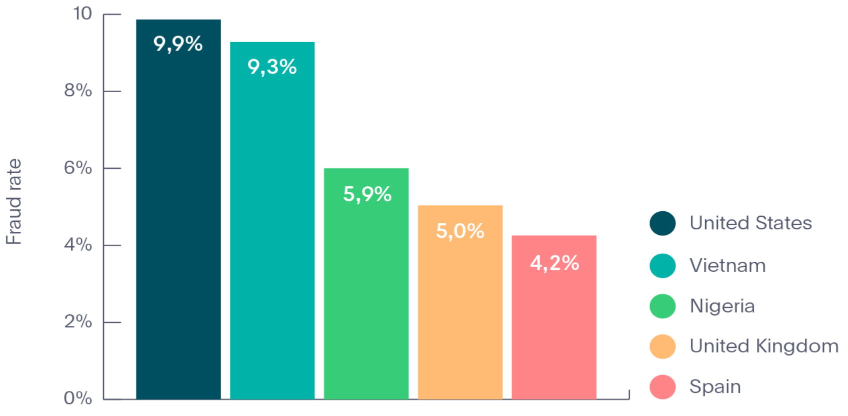
Crypto fraud rate is the highest of the three sectors on a monthly basis and we did not witness any extraordinary jumps during the year the way we did with fintech and mobility (see Graph 3).

Graph 3
Crypto Fraud Rate in 2020



Veriff can verify people from almost anywhere in the world covering more than 190 countries and territories. It's crucial because our clients operate globally. However, when looking at where we see the most online identity fraud attempts globally, we see the United States (see Graph 4) as the leading country with close to a 10% fraud rate.

Graph 4
Top 5 Most Fraudulent Countries in 2020



Here’s a real fraud story from the US that we came across at Veriff:

“We noticed abnormal traffic associated with a car dealership located in the US. In addition to the store’s employees opening crypto accounts and verifying themselves at the spot in the shop, it seemed like shop’s customers were also asked to pose with their documents as a part of the ‘store procedure’. Some of the sessions were guided by what we think was an employee of the shop, some were carried out independently by customers sitting in cars. Unfortunately, this didn’t lead anyone to getting a good discount at the car dealership, but a free crypto account was created on their behalf without their knowledge.”

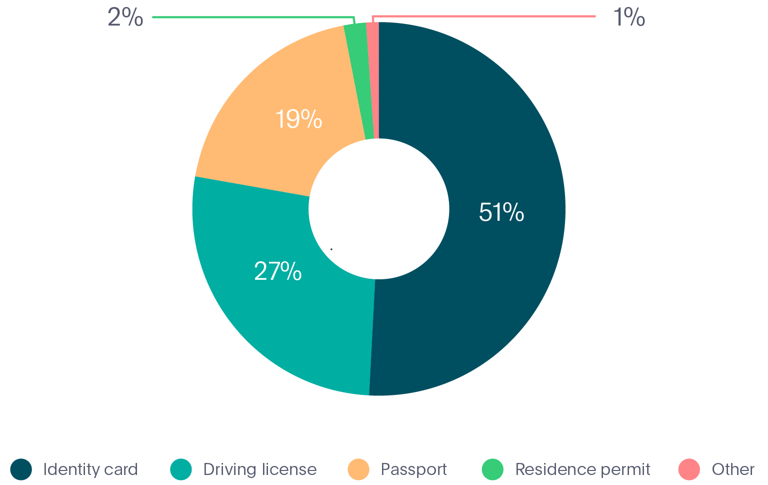
Illustration by Miina Vilo

Fraudsters Love Faking IDs

People use different types of documents when verifying themselves. Veriff supports close to 9,000 different government issued IDs when verifying people, twice as many as our closest competitor. When looking at the document types that fraudsters use the most to illegally verify an identity, we see that over half of them use an ID card (see Graph 5).

Graph 5

Document Types Fraud in 2020

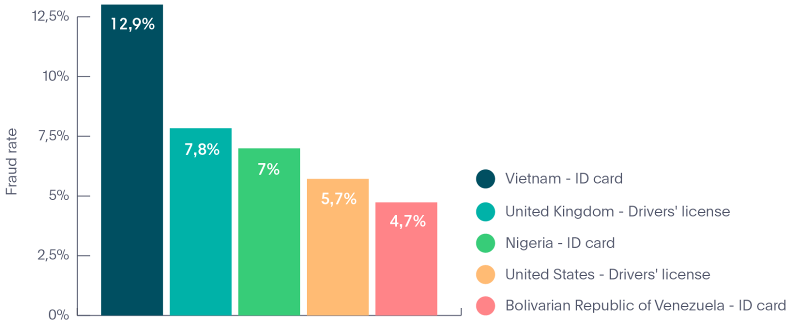


One of the reasons why fraudsters prefer to fake ID cards rather than passports is standardization. Passports hold similar quality and security levels all over the world, whereas ID cards can widely differ regionally. In other words, creating a fake Estonian passport for online identity verification purposes would be around the same level of difficulty as creating a Venezuelan passport. However, when looking at ID cards, a Venezuelan ID card is much easier to fake than an Estonian ID card.

Globally, the top 5 documents that are declined by Veriff as suspected of tampering are Vietnamese ID cards, with a 13% fraud rate, followed by the U.K. drivers' license with 8% (see Graph 6).

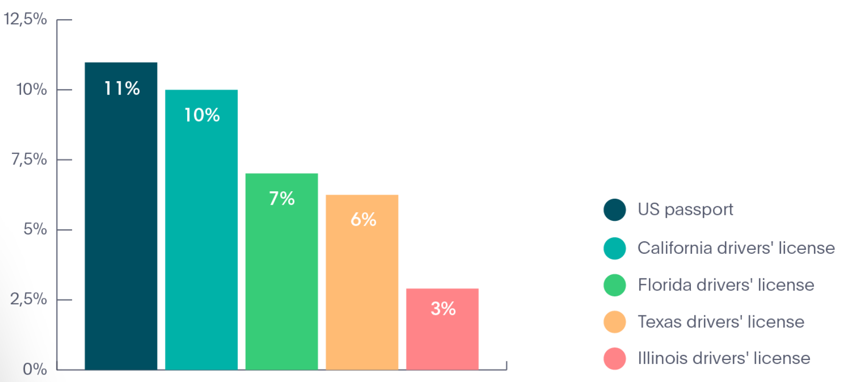
Graph 6

Top 5 Documents Declined as Suspected of Fraud in 2020



However, when looking more specifically into the document types that fraudsters use for identity verification in the USA, the most common one is the US passport (see Graph 7). In other words, the US passport is the document type that is declined the most as being suspected of tampering.

Graph 7
Top 5 US Documents Used by Fraudsters in 2020



In autumn, Veriff launched a barcode scanning feature that enables the company to extract document data automatically, making the process efficient and accurate. A barcode is a standard feature on the back side of all United States and Canadian driver's licenses, making our barcode scanner a secure way to catch instances of document tampering.

Fraud Trends in Different Industries

The fraud that Veriff tackles on a daily basis can be divided into four types.

Table 1
Main Fraud Types

Document fraud	Identity fraud	Technical fraud	Recurring fraud
Tampered documents	Attempted impersonation	Images and/or videos are streamed (or a slideshow)	Velocity abuse
Fake documents	Attempted deceit using fake images	Fruadulent access to the session	

Depending on the industry - crypto, fintech, mobility - the most common type of fraud also varies. Let’s take a look at each industry in more detail.

Fraud Trends in Crypto

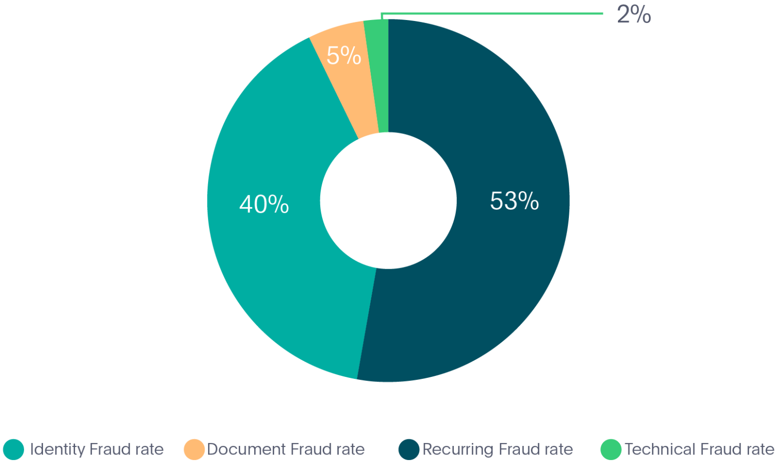
As we mentioned in our Crypto Fraud Report, the cryptocurrency market is subjected to the highest fraud rate month-on-month compared to the other industries that Veriff works with right now. And this trend has remained stable since 2019, when we wrote our first fraud report.

> "
>
> The biggest value that Veriff brings us is the KYC and compliance, where we're removing a lot of the bad actors and stolen IDs. With velocity abuse, where when someone has stolen loads of IDs and they're trying to sign up, Veriff helps us detect where they're coming from and recognizes the repeat use of a device. The benefits of the combination of these tools allows us to reduce the fraud rate and meet our compliance regulations as well.
>
> **Chris Adjei-Ampofo, Uphold's CIO**

uphold

The most prevalent fraud type in the crypto industry in 2020 (see Graph 8) is recurring fraud, making up over half of the fraud attempts. Identity fraud is the second most prevalent type of fraud in crypto. This is more familiar to a wide audience, seeing attackers attempt to impersonate legitimate users with the assistance of fake images.

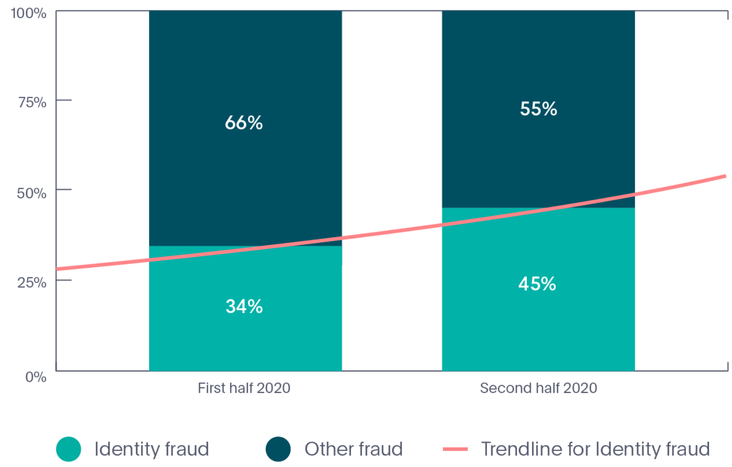
Graph 8
Fraud Types in Crypto in 2020



Here's a true fraud story we came across from Italy. Forging a photo on the document is one thing, but forging the person presenting this document is a whole another story! A guy from Italy has printed out the document with a nicely crafted face on it, and in addition to it he designed a life-like mask matching the identity on the document he was showing. If only he knew we were able to see him 'changing faces', he probably wouldn't have gone this far.

Illustration by Miina Vilo

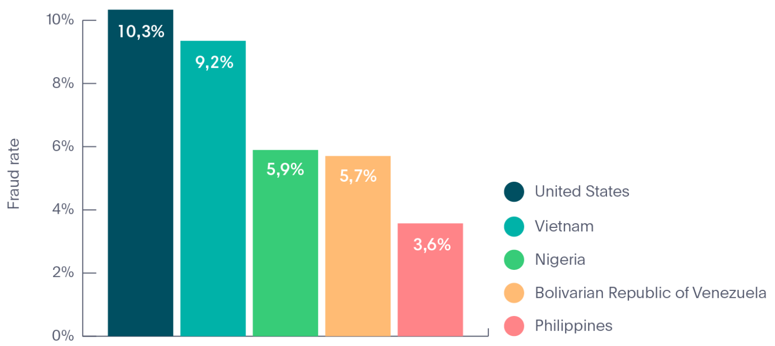
Graph 9
Identity Fraud Rate in Crypto 2020



Compared to the first half of 2020, we've seen an 11% increase in the rate of identity fraud rate in the second half the year (see Graph 9).

As crypto technology is fast-moving and frequently changing, and more and more businesses accept crypto payments, the increase in fraud is not surprising. Fraudsters leverage uncertainty and new procedures enabled by the pandemic, as many people are forced to move more of their lives online and some of them discover online services for the first time. As many people lost economic stability when the pandemic hit, they are now more exposed to so-called 'investment scams', in which criminals convince people to invest into a 'new and developing' cryptocurrency by promising huge turnovers. There were also cases where scammers posing as trusted e-commerce sites were luring customers into buying COVID-19 treatments by only accepting crypto payments. People unknowingly exposed their identities that fraudsters are then re-using for different purposes.

Graph 10
Top 5 Fraudulent Countries in Crypto in 2020



As for the most fraudulent countries in crypto, the US leads the way with over 10%, followed closely by Vietnam and Nigeria. (see Graph 10).

Fraud Trends in Fintech

Fintech services have become an essential part of everyday life for customers and institutions. As more and more services are digitized and clients don't have to physically meet a financial representative anymore to open accounts or perform any financial transactions, the fraudsters' appetite grows together with the fintech companies demand in these times of a global pandemic.

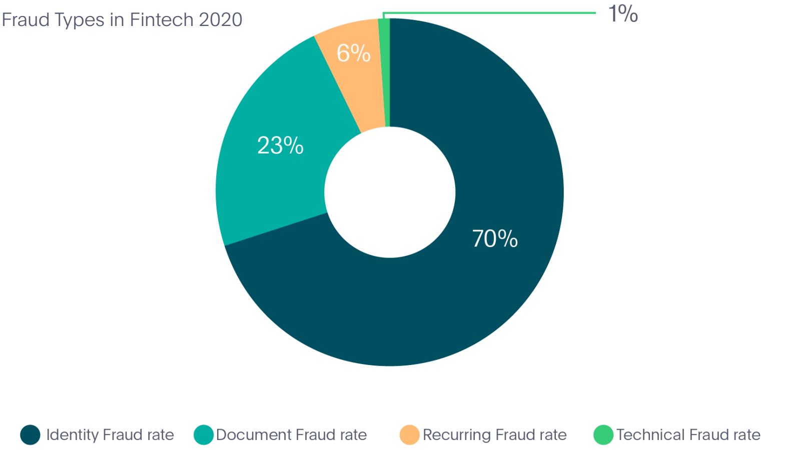
> “
>
> With the help of Veriff's technology, TransferGo is able to verify a customer's identity fast but also in a most secure manner. We are able to prevent any attempts by fraudulent individuals looking to register or use our service. Our partnership with Veriff also supports Know Your Customer (KYC) and Anti-Money Laundering (AML) checks during the initial sign-up process.
>
> **Baran Ozkan, Director of Product**

transferGo

Similarly to crypto, the most prevalent type of fraud in fintech is identity fraud (see Graph 11). With our highly configurable flow and strong fraud prevention Veriff ensures that your business is compliant with all regulations and no fraud slips through the net.

In order to detect whether a verification has been initiated with someone else's physical document, we compare the extracted faces from a selfie and a document photo. If the confidence of similarity is too low we decline the session. If we're not sure, we highlight the appropriate risks and leave the decision for a specialist. If the same user is to submit a different verification attempt in future, we can crosslink the incoming session with the previously declined sessions through face embedding and present risk labels suggesting previous attempts of impersonation.

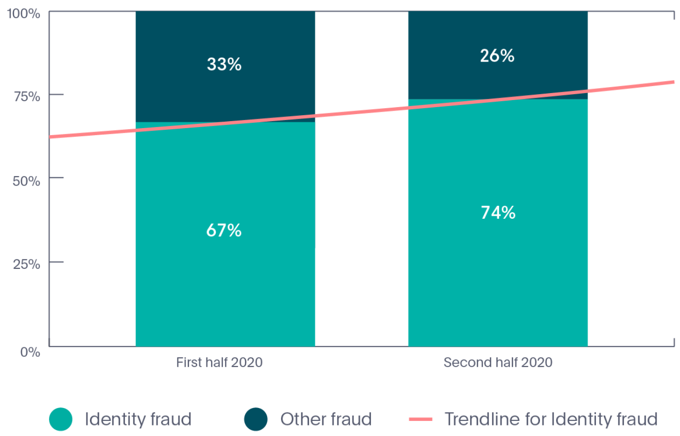
Graph 11
Fraud Types in Fintech 2020



Compared to the first half of 2020 we've seen a 7% identity fraud rate increase in the second half of 2020 (see Graph 12).

New circumstances, additional payment options, and updated procedures (including no longer needing to physically go to financial institutions to perform various verification tasks), have opened up novel opportunities for scammers. There have been more cases of phishing attempts, where scammers pretend to represent banks and ask individuals to provide personal and bank account details.

Graph 12
Identity Fraud Rate in Fintech 2020

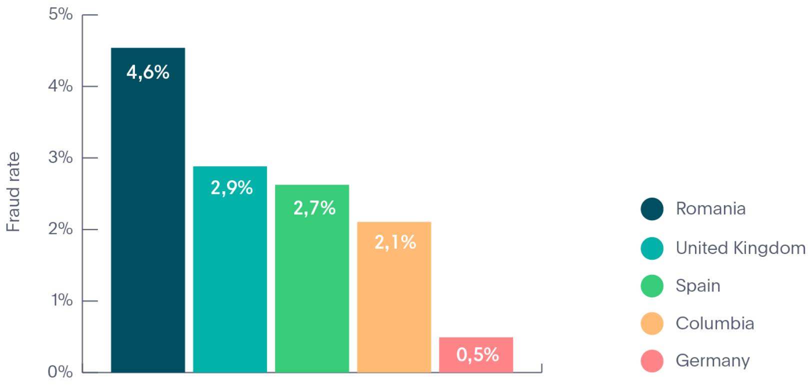


As more people are now working remotely, often using computers that do not have up-to-date software, they are more easily exposed to different malware attacks that would then lead to leaked personal or banking data that fraudsters take advantage of and use on their behalf.

In the fintech sector, the most fraudulent countries come from Europe. With close to 5% Romania takes the lead (see Graph 13), followed by the United Kingdom and Spain.

Graph 13

Top 5 Fraudulent Countries in Fintech in 2020



Fraud Trends in Mobility

Verifying your customer's identity online is an integral part of any business, but when we're talking about mobility, high-value assets are at stake, and you want to know your customer's identity and predict their behaviour before handing them over the keys. And this is where Veriff comes into play by helping you grant access to services to legitimate users, and block potential perpetrators.

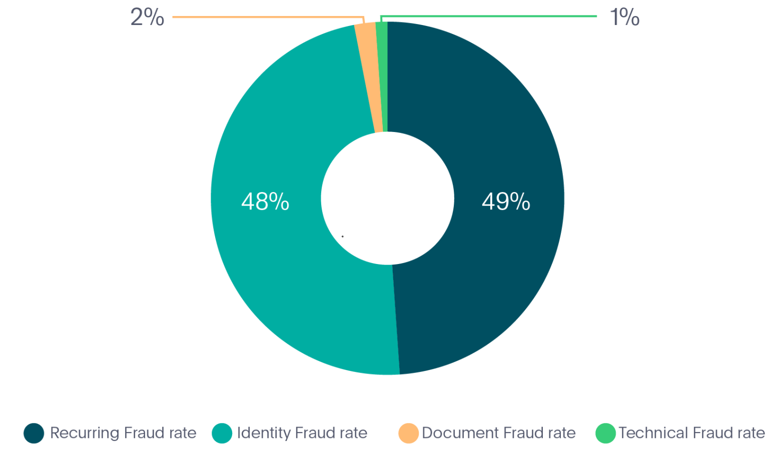
> “
>
> On top of the strong time-saving automation component, we consider Veriff's category extraction feature a game changer, as it fully enables the car-sharing use case. In particular, fraud and damages are an increasing concern in the mobility industry - so of course high cost assets such as a car, or a luxury car for that matter, need to be safeguarded: precise license identification strongly contributes to this.
>
> **Nicholas Kirk, Head of Business Development**

goUrban

In the mobility sector the most prevalent fraud types are identity fraud and recurring fraud, which are almost equally divided (see Graph 14).

If fraudsters manage to abuse the system, they will come back and try again. And if they fail to do so, they will still come back - and try twice as hard. But luckily, recurring fraud is where Veriff's crosslinks shine the brightest. If we're confident that the end-user has committed fraud before, we'll automatically decline all the recurring attempts associated with the same person, device, or document.
If the same person, device, or document, have been found approved in the historically submitted sessions, all the recurring attempts will be declined with Velocity/Abuse - a feature that ensures that no end-user abuses your service via multi-accounting.

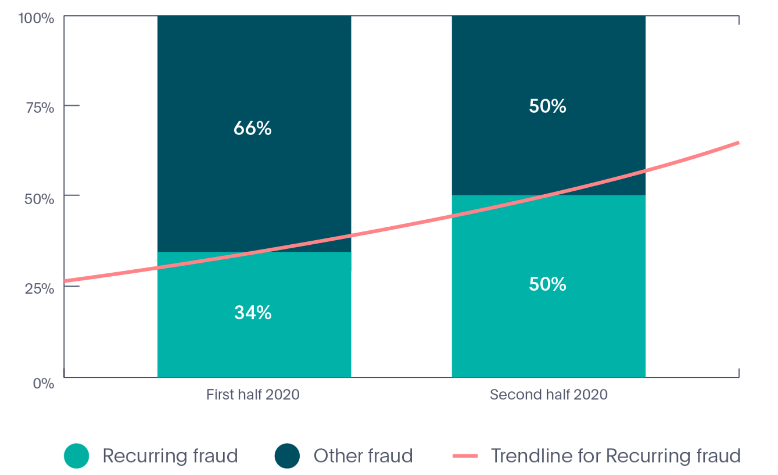
Graph 14
Fraud Types in Mobility



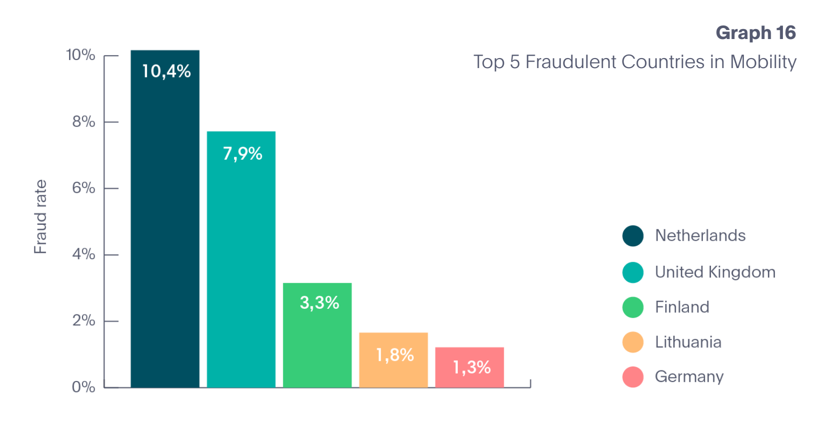
Compared to the first half of 2020 we've seen a 16% increase in recurring fraud rate in the second half of the year (see Graph 15), which pushed down identity fraud to the second most prevalent type of fraud in mobility.

As the use of scooters skyrocketed in many cities because of the pandemic, the increase in fraud is expected. We've seen many cases where underage users are trying to get access to vehicles with someone else's document or showing an official document specimen from their devices, and then getting looped in auto declines.

Graph 15
Recurring Fraud Rate in Mobility in 2020



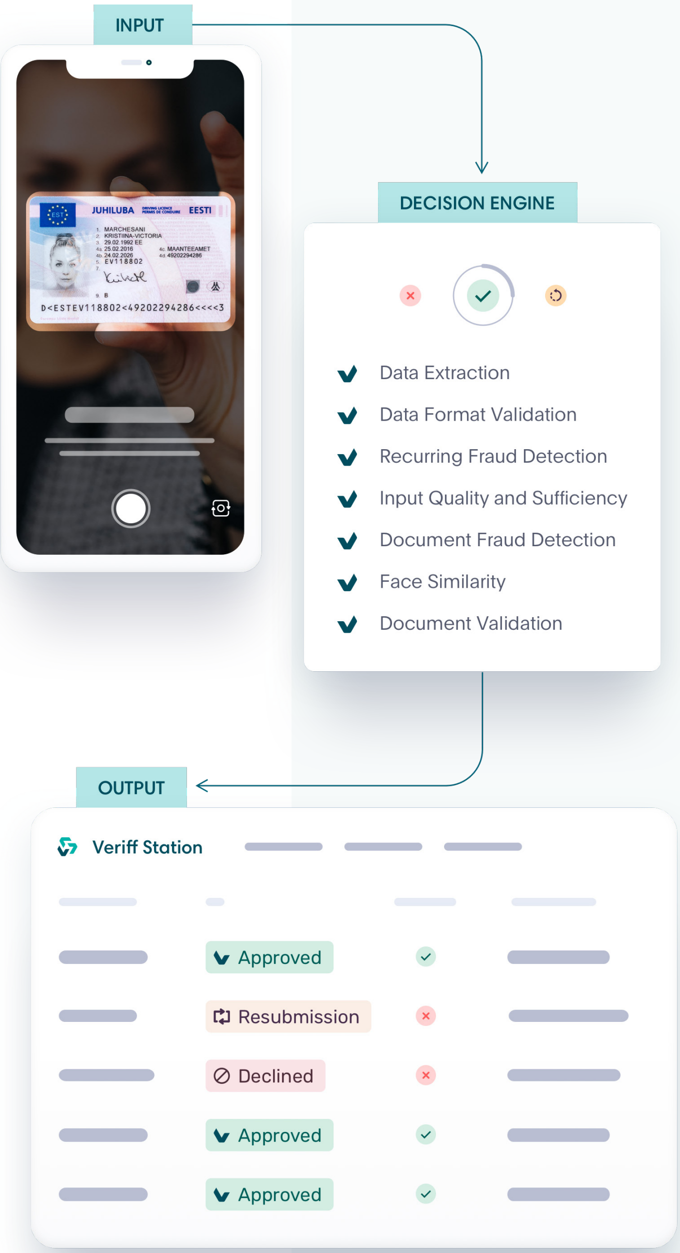
When we're looking at the countries where fraud is most prevalent in the mobility sector, we see Netherlands in the first place with over 10% fraud rate (See Graph 16).



Graph 16
Top 5 Fraudulent Countries in Mobility

How Veriff Detects Fraud

It takes much more than just making sure that two pictures match - it needs an intelligent decision engine to detect fraud. You can't even trust your own eyes - people are subjective by nature and make mistakes when handling large amounts of data. To escape that, Veriff has built an in-house intelligent fraud prevention engine (see Image 1) that is automating the decision-making process and assists specialists in case an automatic decision can't be made or is inconclusive. We leverage device, network, and customer behavioural information, all as part of our video-first approach.



- ✓ Data Extraction
- ✓ Data Format Validation
- ✓ Recurring Fraud Detection
- ✓ Input Quality and Sufficiency
- ✓ Document Fraud Detection
- ✓ Face Similarity
- ✓ Document Validation

✓ Approved
Resubmission
Declined
✓ Approved
✓ Approved

Image 1
Veriff's Decision Engine

The fraud prevention engine can be broken into smaller pieces but all of them revolve around our proprietary device and network fingerprinting solution.

Crosslinking

Crosslinking allows Veriff to group together sessions that share similar data points. Based on previous knowledge, fraudsters don't tend to limit themselves to one try - they'll try to get verified today, tomorrow and in the upcoming months and they won't stop as long as they have fake identities available to them. All the information from crosslinks is taken into account by our automatic decision engine, and is forwarded to our clients.

Velocity/Abuse

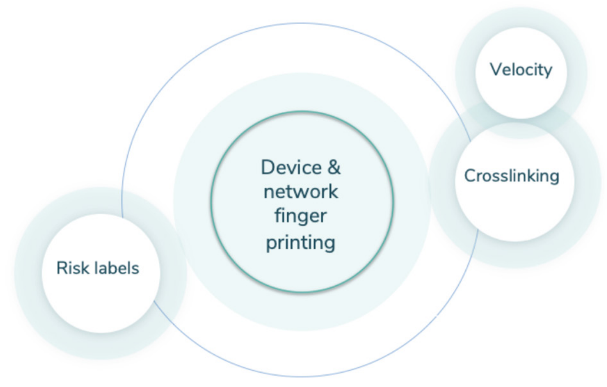
Velocity/Abuse ensures that no end-user abuses your service via multi-accounting. Taking into account all of the information we see through crosslinks, we can automatically shut down users if they, their document, or device have been approved before. We have three velocity checks that can be activated altogether or independently from each other:

Duplicated user
checks whether the person has been approved before

Duplicated document
checks whether the document has been approved before

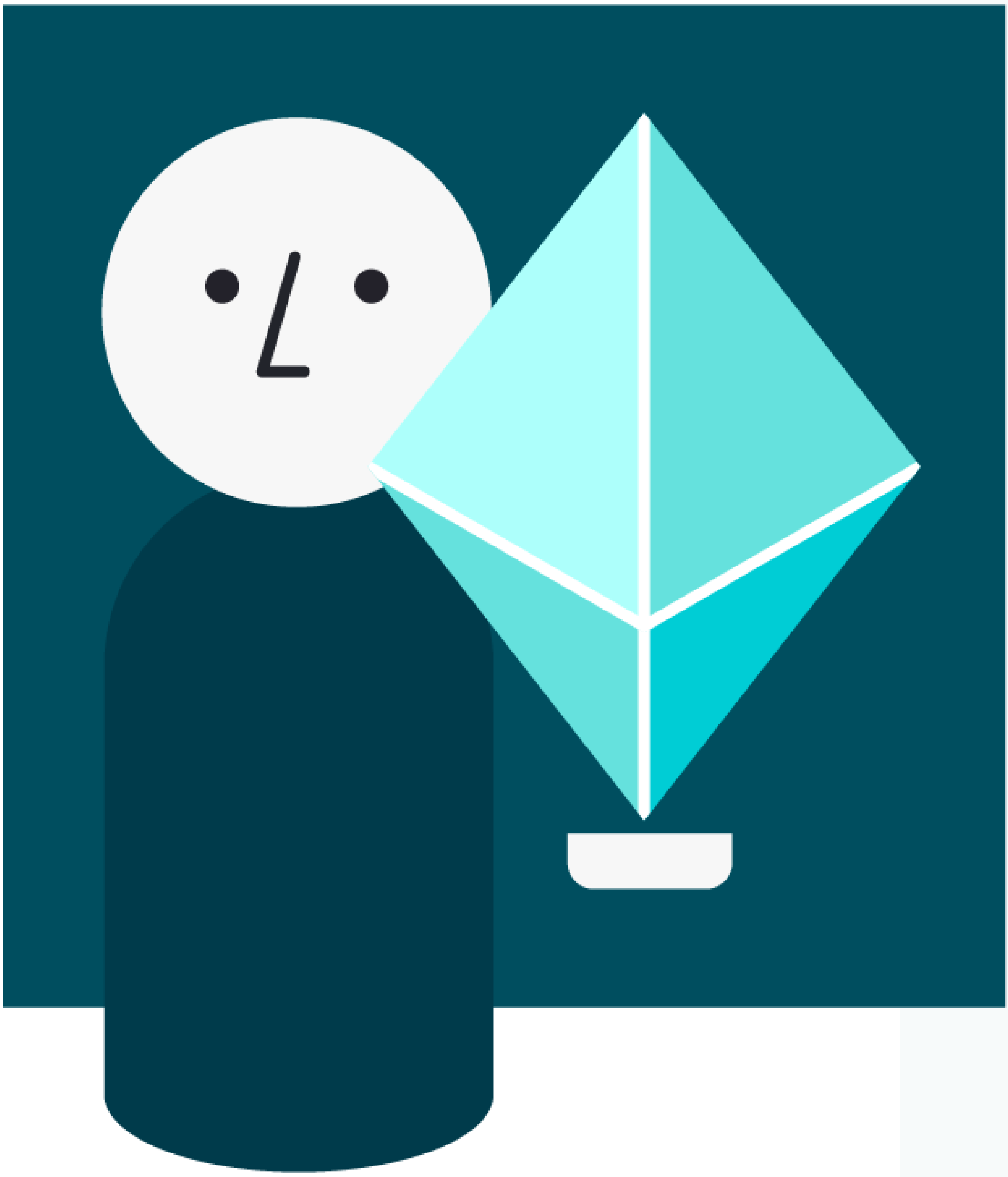
Duplicated device
checks whether the same device has been approved before

Image 2
Veriff's Fraud Prevention Engine



Risk labels

Risk labels point out the signs of fraudulent behavior in sessions. These labels are used by our specialists in more detailed security reviews and are forwarded to clients to give insight about the final decision and help in post analysis.



Veriff's Recommendations

Crypto

Because cryptocurrency is built on the principles of anonymity and decentralization, introducing identity-based security measures might be faced with high resistance. However, Know Your Customer (KYC) compliance laws will soon apply to many forms of cryptocurrency services, particularly exchanges and wallet services that include the use of fiat currencies.

With the regulatory environment gaining momentum, it is recommended that cryptocurrency and blocktech companies implement identity verification as soon as possible to minimize the friction that will occur as a result of the transition.

Fintech

With the majority of fraud cases identified through live video activity, the fintech industry must be particularly vigilant when it comes to preventing identity fraud.

Account takeover fraud, in particular, is a high risk, and less secure methods such as one-time passcodes do not adequately prevent cases of coerced or suspicious logins.

Mobility

As the mobility sector continues to shift focus away from production and moves towards more service-based business models, account security and anti-fraud practices will become increasingly important.

Continuously monitoring fraud cases and adapting security measures accordingly will play a huge role in maintaining these low rates in an industry that is growing fast, especially because of the market translation caused by the Covid-19.

Keep your eyes on our blog and social channels for more news in identity verification and fraud prevention tips.

Talk to us

If you'd like to learn more about Veriff's fraud prevention technology, you can visit our website or contact us via sales@veriff.com.

veriff.com