Shufti Pro

GLOBAL ID FRAUD REPORT

2021

CONTENTS:

FOREWORD

We are surprised to see the remarkable turn of fraudsters from simple manipulation of identity documents to tech-driven tampering to dodge identity verification. As we move on to 2022, I would advise businesses in every industry to employ robust mechanisms to combat identity thieves and financial criminals.

VICTOR FREDUNG

Advanced technology is not only helping businesses but imposters too. Fraudsters used AI to tamper with government-issued identity documents for dodging identity verification. As criminals are leveraging advanced technology for their illicit gains, organizations are at stake and need robust measures to combat bad actors.

SHAHID HANIF

ABOUT SHUFTI PRO

Shufti Pro has a global audience of end users from 230+ countries and territories. We spent years refining our AI to mitigate advanced fraud. Below are some points to best describe Shufti Pro and its services.

Hundreds of businesses onboarded

150+ languages supported

3000+ identity documents

Millions of end-users

Several global awards

Thousands of AI models

5 global locations

92% customer satisfaction rate

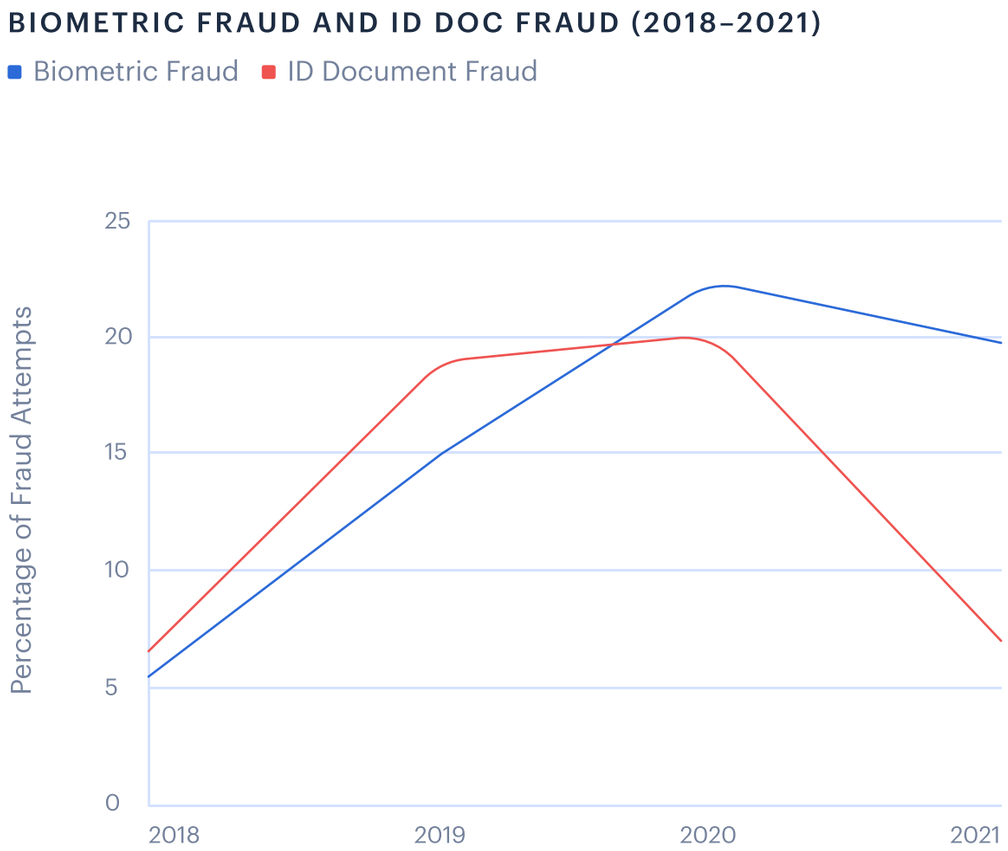
Globally configurable KYC/AML compliance services of Shufti Pro are equally beneficial for businesses from finance and crypto to gaming and gambling industries. Biometric verification, ID document verification and age verification services of Shufti Pro are some of its highly demanded services around the globe. The new addition of on-premises identity verification in the services hub is the highly sought-after product in the banking and finance industry.

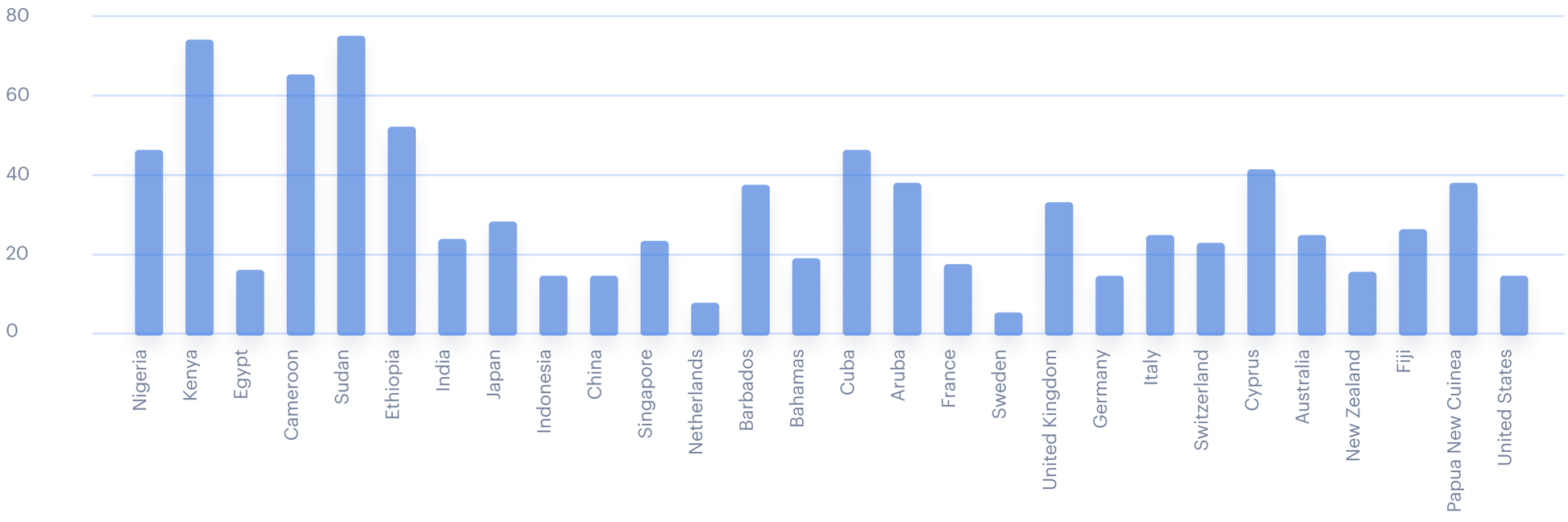
With increase in demand, we encountered rising fraud attempts of sophisticated fraud during 2021. Read this report to have detailed insights on global fraud trends, industrial outlook of IDV fraud and 2022 predictions. For regular insights about identity verification, biometrics and KYC/AML landscape ***subscribe to our newsletter***.

Please give proper credit to Shufti Pro when quoting any part of this report.

QUICK LOOK AT 2021

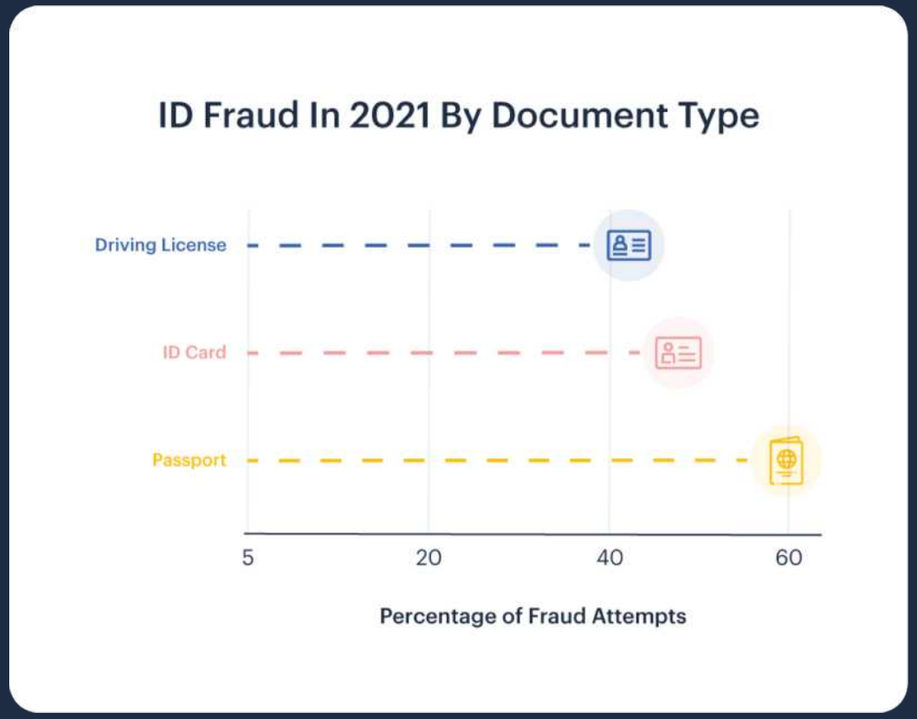
The year 2021 was all about fighting the rising number of biometric identity frauds and facing more rigid identity verification and background screening regulations across the globe. Experts of the Shufti Pro team predicted a rise in biometric identity frauds, synthetic identity theft in its ***Global Identity Fraud Report 2020.*** Unfortunately, all of these were true and organizations worldwide reported a significant rise in these scams.





In 2021, Sudan, Kenya, Cameroon, and Ethiopia were the primary targets of fraudsters with biometric fraud attempts surpassing **50%**.

On the other hand, **identity document** fraud attempts increased, with passports being the most tampered document in 2021.



IDENTITY FRAUD - THE GLOBAL INDUSTRIAL OUTLOOK

Over the years, almost every industry across the globe has accepted the importance of identity verification to combat identity theft, account takeover fraud, phishing attacks, etc. along with effective compliance with the changing KYC/AML landscape. Although the finance industry has been complying with the customer due diligence (CDD) regulations the longest, laws for this sector have also become more rigid, thanks to the whopping increase in criminal activities. On the contrary, the crypto sector is now the prime target of regulatory watchdogs. Law making authorities are paying more attention to the cryptocurrency sector ever since criminal activities through digital assets increased.

Among all the industries Shufti Pro witnessed the highest fraud rate of **43%** in the Finance industry.

BANKING AND FINANCE

Just like 2020, the banking industry was on the radar of cybercriminals in 2021 as well. The COVID-19 Pandemic has created ideal conditions while opening doors for fraudsters to exploit digital channels. According to the ***UK Finance Report***, criminals stole around **£754 million** through fraud from the finance industry alone in the first half of 2021 - 30% more than the same period in 2020.

To thwart identity theft, money laundering, terrorist financing and proliferation financing regulatory bodies are more vigilant than ever.

Tranche 1.5 reform introduced by AUSTRAC calling for advanced customer due diligence protocols to combat ID fraud and financial crimes in the region

FinCEN, for the first time, issued government-wide guidelines to combat money laundering, terror financing and criminal activities that are on the rise

DO YOU KNOW ?

In the first half of 2021, the banking sector has been fined a total of **$937.7 million** for non-compliance with KYC, AML and data privacy regulations.

With Shufti Pro's globally compliant KYC/ AML solution stay ahead of fraudsters and financial criminals. Let Shufti Pro be your trusted partner in swift customer onboarding through AI-powered identity verification and AML checks.

Sopra Banking Software is reducing compliance costs in partnership with Shufti Pro

Read Details

CRYPTOCURRENCY

In 2021, the crypto sector experienced increased retail and institutional interest that eventually led to higher fraud rate and millions of losses for investors. According to Chainalysis, crypto crimes hit an all-time high of **$14 billion** in 2021. These crimes involved scamming being the greatest form followed by crypto theft.

GLOBAL CRYPTOCURRENCY THEFT ROSE TO 516% FROM 2020

Source: CipherTrace, Chainalysis

After a surprising turn of events in the crypto sector in 2021, regulatory watchdogs have decided to reduce anonymity and ensure effective measures to combat money laundering and terror financing activities through crypto.

An AI-powered solution is what the industry needs for unintentional contribution to financial fraud in the crypto industry, and as one of our partners, ACE said,

DO YOU KNOW ?

In 2021, 72% of the stolen crypto funds were taken from DeFi protocols.

With sound policy and our business alliance with Shufti Pro, we want to prevent unknowingly contributing to financial and economic crime.

Samreen Vos,
compliance officer of ACE

Read Details

NON-PROFIT AND CHARITIES

Amid COVID-19 Pandemic, people are seen stepping forward more than ever to help the world, especially during the holiday season, providing fraud opportunities to troublemakers. Charities and fundraising activities are no longer safe from money launderers and fraudsters.

According to figures from the Charity Commission, 65% of charities feel that COVID-19 pandemic has increased the risk of fraud due to digital sign-off processes.

DO YOU KNOW ?

The most common charity frauds reported by organisations are unauthorised fundraising and credit card scams. Apart from that financial criminals are actively taking advantage of NGOs to fulfil their illicit gains.

In November and December 2021, countries have stepped forward with the idea of ***identity verification*** and AML screening of donors. Shufti Pro's configurable KYC/AML solutions let organisations ensure that illegally earned money stays arms away from charities and fundraising activities.

Read Details

FINTECH

The world is diving deeper into the digital world and FinTechs are gaining prominence. Nevertheless, the loopholes in the current regulatory regime and customer due diligence protocols resulted in a war between perpetrators and fintech companies.

In 2021, the FinTech industry soared with a record of ***$91.5 billion*** in global funding, almost twice in number as compared to 2020.

DO YOU KNOW ?

In the first half of 2021, identity verification fraud rate across fintech sectors spiked 15%. Meanwhile, the insurance sector secured **$1.3 billion** using AI solutions. Companies that adopt digital client onboarding solutions and ensure legitimate customer onboarding are able to avoid hefty non-compliance penalties - just like Opal did by opting for Shufti Pro.

"Shufti Pro helps us ensure our customers experience a fuss-free pleasant experience at the onboarding stage. It set us up in the right direction to provide our customers with additional positive experiences when they subsequently perform their transactions with us"

Lim Ming Wang

CEO and Co-founder of Opal

Read Details

ONLINE DATING PLATFORMS

Catfishing, romance scams, and money muling attempts are very common in the online dating industry. Why? Because there are no stringent regulations to combat criminals. Fraudsters take complete advantage of the vulnerability and target people looking for their perfect match.

In ***March 2021***, the use of the Hinge messaging app increased by 30%, Tinder had over 3 billion swipes in a single day, and virtual dates on OkCupid increased by 700%.

DO YOU KNOW ?

According to the Wells Fargo 2022 study, 63% of online daters have been contacted by a scammer. All this due to lack of proper identity verification and screening checks. Online dating industry needs a multi-layered AI-powered solution to combat catfishing and romance scams.

In 2021, DateID partnered with Shufti Pro to secure its platform through a smooth process, resulting in a threefold increase in customer acquisition rate.

"IDV is not as simple and straightforward as you'd think. Shufti Pro's UX is very well-thought-out compared to some other platforms we tested."

Remy Tennant

the founder of DateID

Read Details

GAMING AND GAMBLING

Gaming and Gambling industry is expected to grow to $74 billion by 2023. With growth comes the risks. This massive flow of money on gmabling platforms is attracting criminal entities. The Australian authorities received 6000 gambling ***scam reports*** in the first quarter of 2020.

During 2021, fraudsters were witnessed creating multiple accounts on betting and gaming platforms using fake and synthetic identities.

DO YOU KNOW ?

UK Gambling Commission imposed a penalty worth ***$10 million*** on a gambling company for not having adequate KYC procedures for player verifications.

With over 2 billion gamers online, around 60% of the traffic on the platforms is cross border. It makes it challenging for the operator to successfully regulate the gaming and gambling industry and comply with ever changing KYC/AML regulations.

This sector can reap numerous benefits from globally configurable automated ID verification systems like Shufti Pro. It not only enables them to comply with KYC, AML and age laws but also prevents identity fraud in real-time.

Learn More

RIDE SHARING

Over the past years the ride-sharing industry has gained traction, opening new doors for fraudsters to exploit user identities. Millions of trips are completed by the ride-hailing apps, and security remains a critical concern for both drivers and passengers.

According to the ***Metropolitan Police Officer***, approximately 3 million riders and over 40,000 drivers who regularly use Uber have been witnesses to serious ride-sharing crimes and incidents in London.

DO YOU KNOW ?

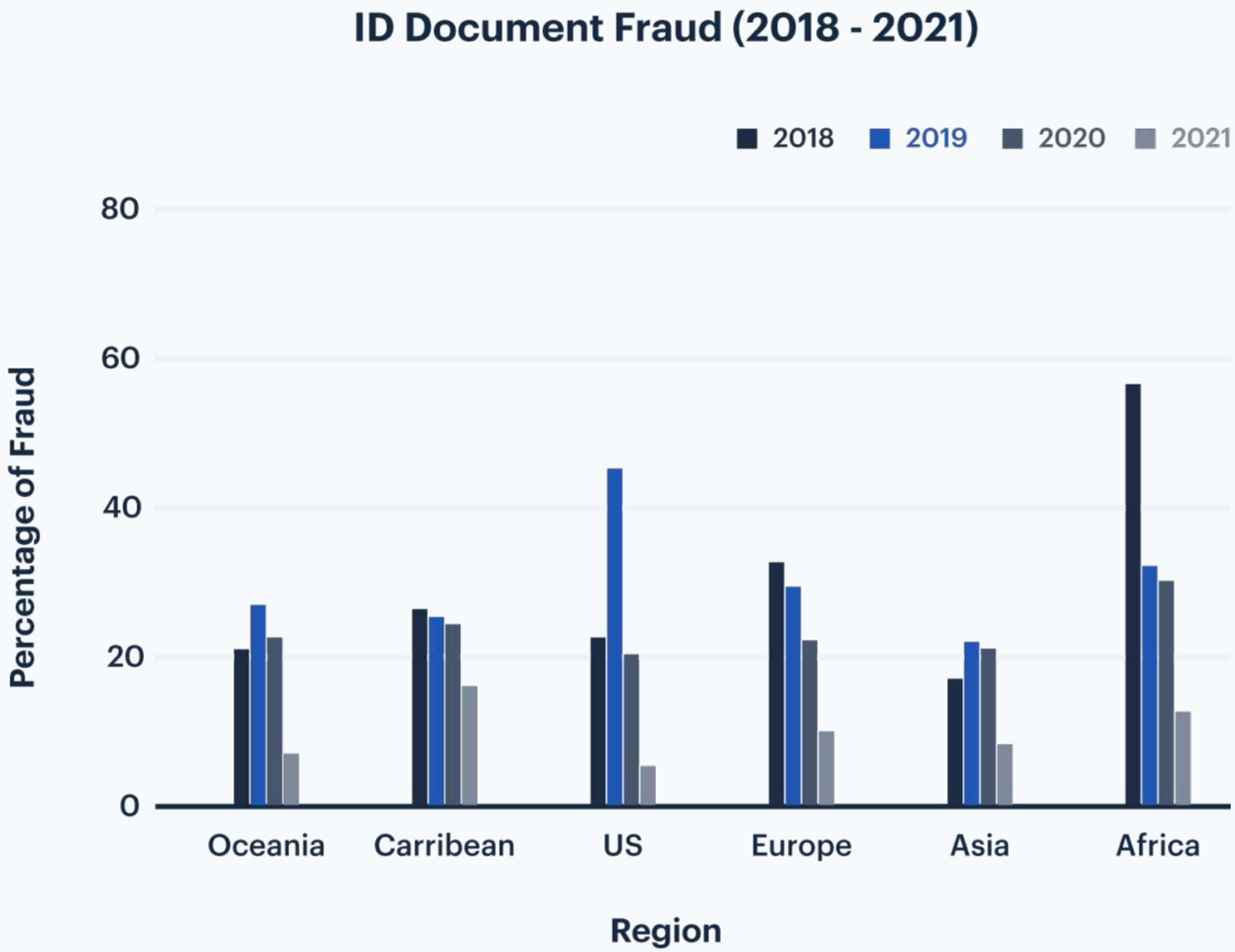
Last year scammers allegedly earned ***$195,000*** by referring fake drivers to delivery apps. It is reported that the scammer created around 487 fake accounts using stolen identities and then sold those accounts to unqualified drivers. The reason local governments are enacting a slew of rules aimed at regulating ride-sharing service providers.

Ride-sharing apps can avoid such frauds by putting enhanced identity checks in place during account creation for both passengers and drivers. Shufti Pro's multi-layered approach to verify user identities in real-time leaves no room for identity fraud while offering a seamless onboarding journey.

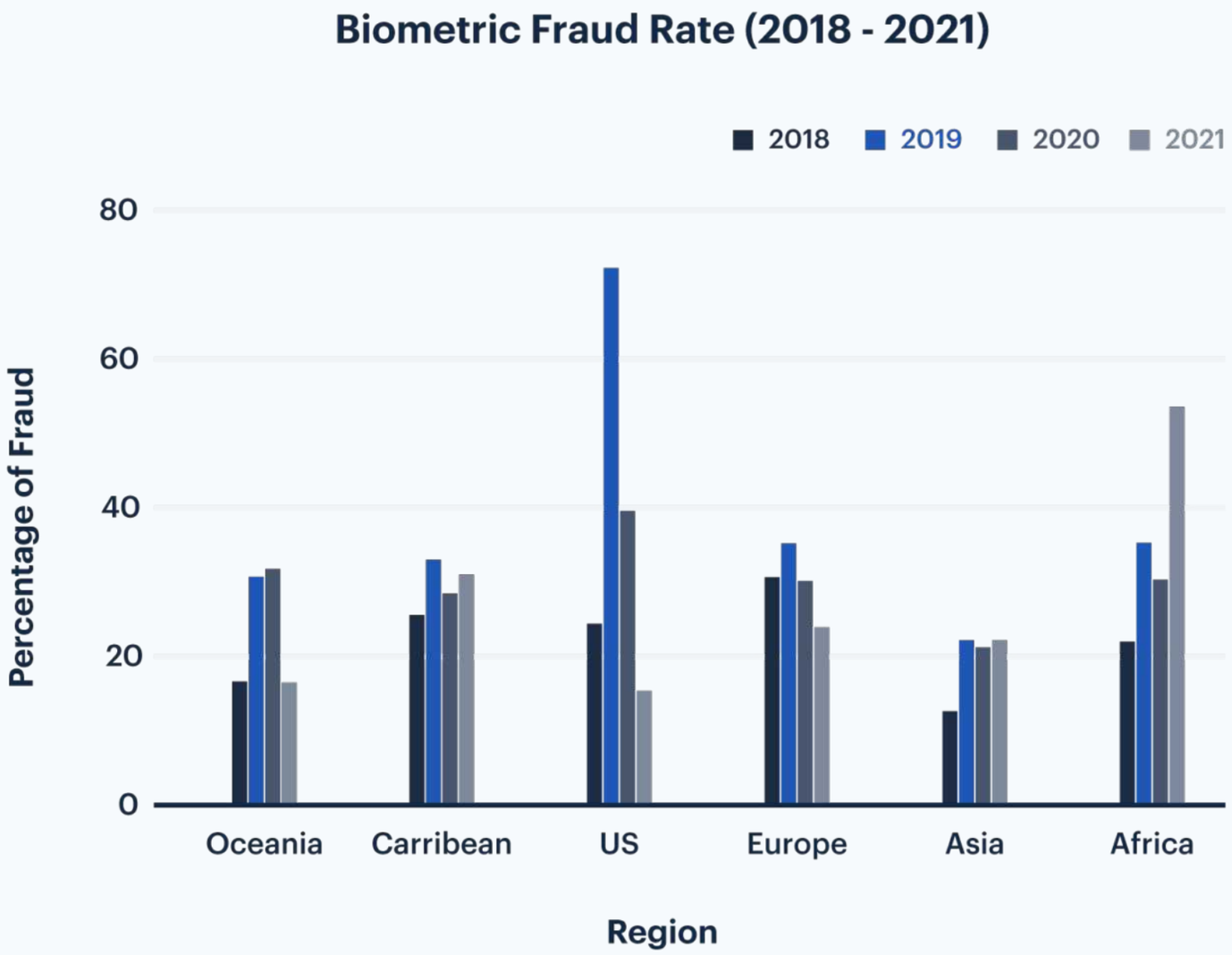
Learn More

FRAUD ANALYSIS

Since the establishment of Shufti Pro, the company has experienced an interesting turn of events when it comes to frauds. We've seen a spike in fraud attempts using government-issued identity documents. However, the uncertain fraud situation in every region of the world is demanding more robustness in the end-user verification system.



Despite the stringent regulations, perpetrators managed to achieve their goal. When businesses were struggling to combat ID document fraud rates, they were working on manipulating biometric identity verification protocols. Henceforth, the corporate sector saw a significant rise in spoof attacks, digital replay attacks, deep fakes, and various other fraudulent activities during the pandemic.



DITCHING THE 9 – 5 FRAUD CYCLE

Due to the coronavirus pandemic, every company wholeheartedly embraced the remote working option. Surprisingly, criminals are not working 9 - 5 and use the slow working hours and weekends to surpass the security thresholds. At Shufti Pro, we have experienced an increase in fraud attempts during the holiday season. During the holiday season most of the employees are on holidays which reduces security levels in companies that perform manual identity verifications. Integrating an AI-powered solution is what the companies need to cater fraud during holiday season and peak hours of the day.

Some of the biggest scams in history occurred on weekends. Back in August 2021, the ***biggest theft in the history of crypto*** scams was reported by Poly Network. Hackers managed to steal USD 600 million on August 10, 2021 (Sunday) and returned half of the amount on August 12, 2021.

WHEN FRAUD IS AT ITS PEAK

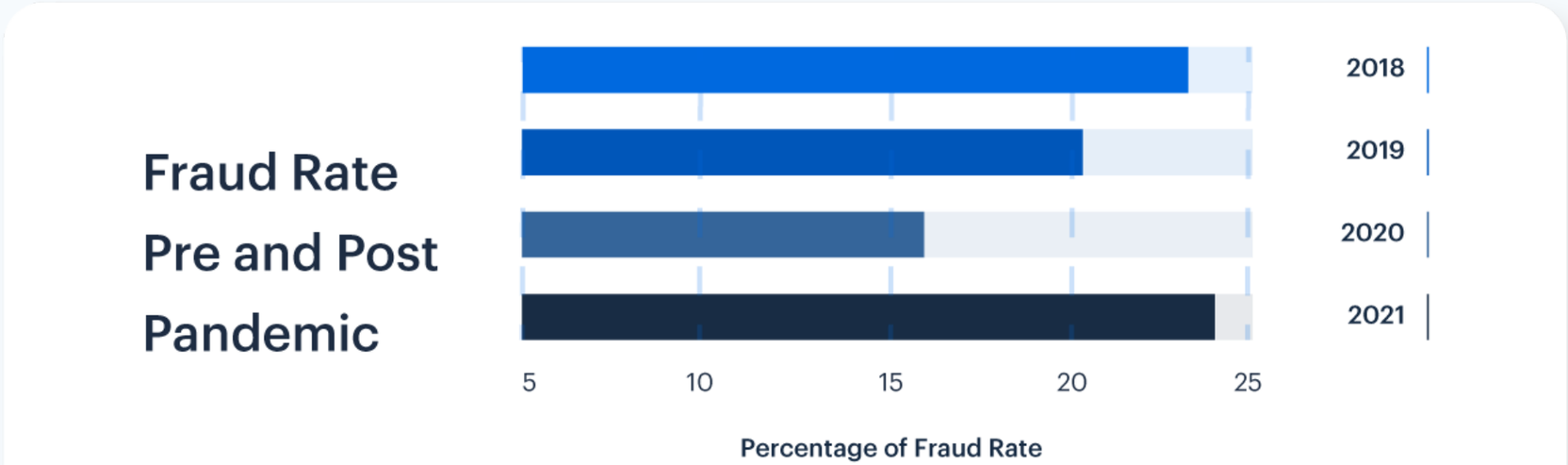
Higher fraud attempts are witnessed between 10am to 3pm.

Biometric fraud during the holiday season is around 5% more than the fraud rate in the whole year.

THE POST-PANDEMIC FRAUD RATE IS INCREASING

While reviewing the fraud trends before, during, and after the pandemic, Shufti Pro's analysts are surprised to see the rise in criminal activities post-pandemic. Moreover, there are no chances of reduction in the near future.

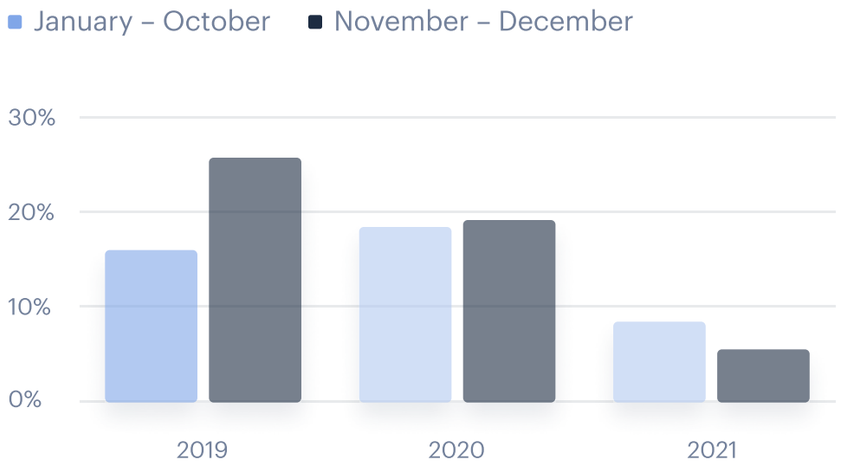
According to Shufti Pro's findings, the post-pandemic situation of fraud is not at all favorable for businesses across the globe. Bad actors fully utilized the worsening Covid situation and used advanced technology to tamper with identity documents and come up with new spoof attempts. The overall fraud rate was approximately 21% in 2020 and by 2021, a whopping 3.35% increase was observed.



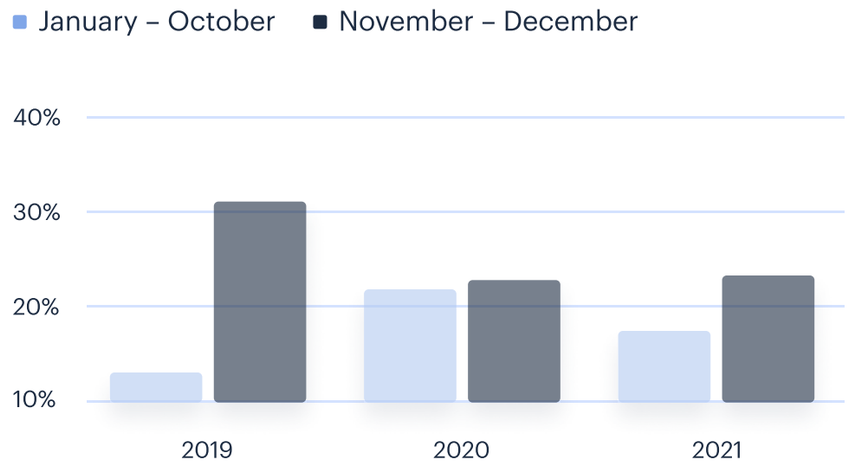
HOLIDAY SEASON – PRIME TIME FOR ID THIEVES

Holiday season is the perfect time for criminals to target businesses and individuals for their illicit gains. Thanks to the Covid-19 pandemic and recurring lockdowns, perpetrators have figured out better ways to dodge identity verification systems. Impersonation scams, synthetic identity fraud, account takeover fraud, new account fraud, and chargebacks were some of the most encountered fraud attempts this holiday season.

ID DOCUMENT FRAUD DURING HOLIDAY SEASON



BIOMETRIC FRAUD DURING HOLIDAY SEASON



NEW MANIPULATION TECHNIQUES ENCOUNTERED IN 2021

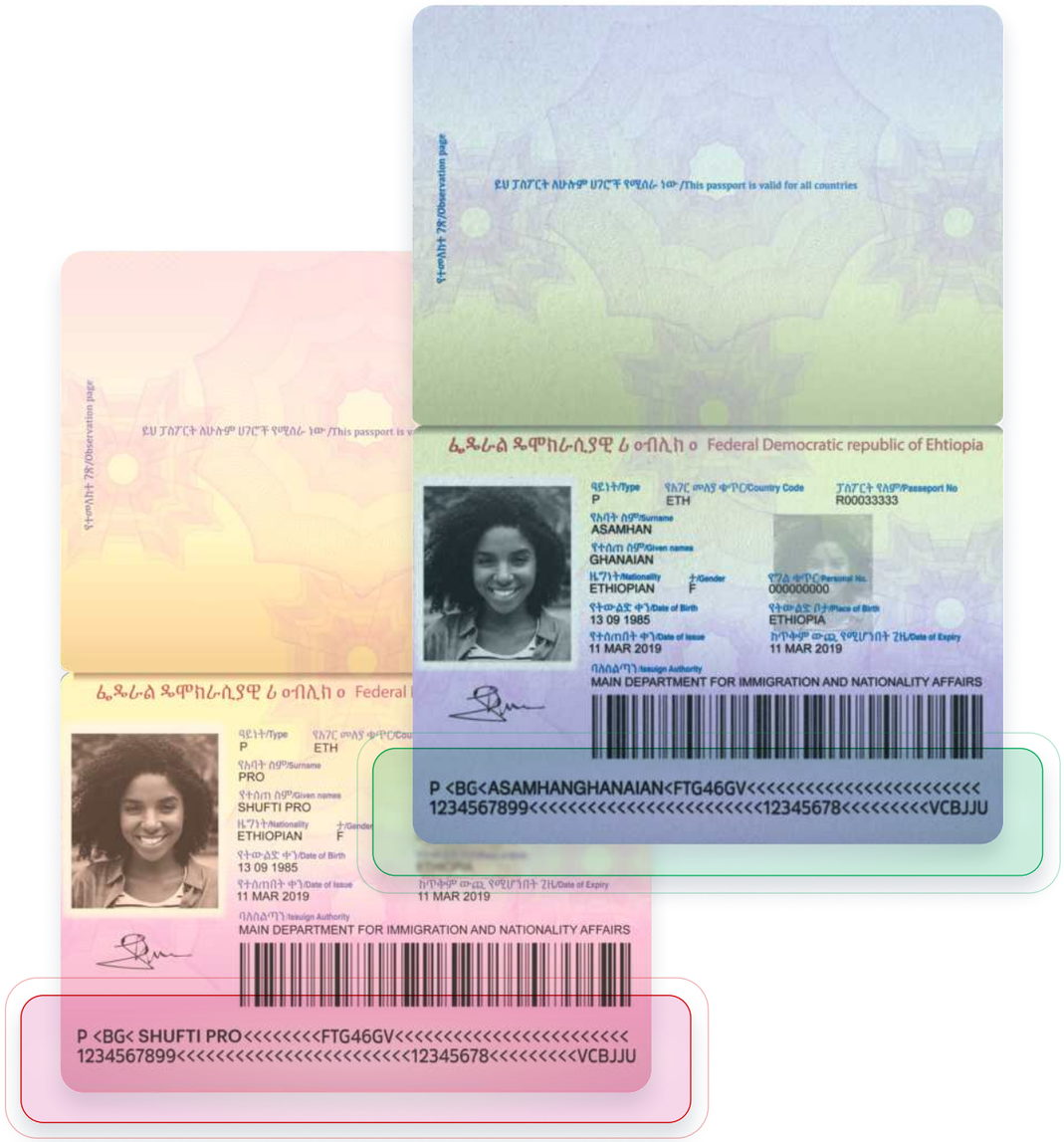
During identity document verification in 2021, various new manipulation techniques were highlighted that took our experts by surprise. First of all, passports have been widely used for identity verification and the fraud attempts revolved around manipulation with the **MRZ code.**

Why passports anyway? Well, passports are considered to be one of the most legitimate sources to verify one's identity. National Identity Cards are not designed for international travel and the majority of security checks depend upon passports. Instead of manipulating an ID card to dodge the verification checks, fraudsters find it easier to mess with passports and use it anywhere they want.

MRZ MANIPULATION

Altering the MRZ code of any identity document is one of the sophisticated fraud techniques. Minute alterations within MRZ code are settled in such a manner that it is near impossible to track for systems that lack models trained on real data of identity documents. Having spent years in exposure to identity fraud our AI is trained on sufficient real data models that it identifies these minute alterations of MRZ code in mere seconds, saving our customers from fraud and financial loss.

Not to mention MRZ is just one of the multiple checks that Shufti Pro performs on identity documents in real-time, and that too in seconds. Read more about our Document Verification Service ***here***.

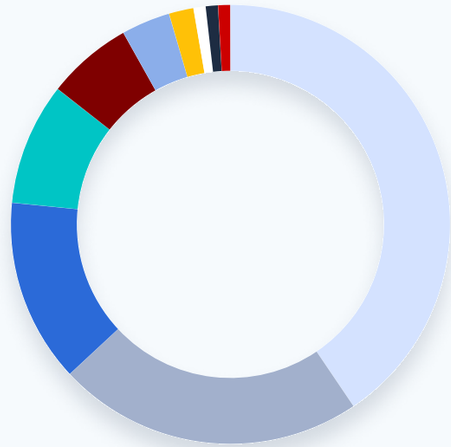


NEW ID DOCUMENTS = MORE SOPHISTICATION

Fraudsters are more in favor of starting from scratch than bearing the challenges of tampering with one or two elements of the identity document. The majority of the ID document verification requests we receive fail because counterfeit documents cannot pass through our system at all. Downloading a free template and then messing with a few fields to reproduce a new identity document is chosen above all which gives us an edge. For an AI-powered document verification system, it is not a problem to detect such attempts.

In 2021, Shufti Pro captured around 33% fraud attempts and surprisingly, the identity documents were tampered.

MOST ENCOUNTERED FRAUD ATTEMPTS IN 2021



- Document originality
- Image manipulation
- Face unmatched
- The uploaded image of the document is blur
- Address did not match
- Face could not be verified
- Name on the document doesn't match
- Document proof tampered
- Front and backside of the doc manipulated
- Name on the Address Document doesn't match

SCREENSHOTS

Screenshots increase the chances of identity fraud when the end-user uploads the screenshot of a document or face to mimic real-time photo upload. But such frauds can be easily catered through AI-powered services of Shufti Pro. In 2021, 5% identity documents uploaded during verification were screenshots.

PHOTOSHOPPED ID DOCUMENTS

This year, Shufti Pro detected more than 5% increase in photoshopped identity documents. Photoshopped documents have forged images, altered personally identifiable information (PII) and these edits are hard to detect with naked eye. However, Shufti Pro's AI-powered document verification detected these fraud attempts in less than a second and assisted businesses in combating identity document fraud.

EXPIRED ID DOCUMENTS

Shufti Pro's algorithm does not accept expired identity documents since the majority of fraudsters bank on expired documents for their ill gains. Our system is set according to the regulatory requirements of every state. Be it a said expiration date by law, mentioned on the identity document, or punched by the government, Shufti Pro's AI can authenticate the validity of the document. This year, fraud using expired/punched documents skyrocketed and accounted for 49% identity document fraud.

SCANNED ID DOCUMENTS

Did you know the probability of fraudulent activities significantly increases if the uploaded documents for verification are scanned? Around 35% of fraud attempts were made through scanned ID documents.

BROKEN/CROPPED ID DOCUMENTS

As an attempt to manipulate the identity verification system, imposters repeatedly use cropped images of stolen identity documents or broken ID cards. With 98.67% accuracy Shufti Pro's Know Your Customer (KYC), 5% of fraud attempts through broken and cropped ID documents was detected in 2021.

TEMPLATE MATCHING

Multiple platforms on the dark web are supplying templates of identity documents that are closer to real ones. Fraudsters use these templates to develop fake or synthetic identities which are near impossible to identify in manual verifications. Our systems are trained to identify new fraud techniques through artificial intelligence and template matching is one of the new fraud techniques we captured in 2021.

REPLAY ATTACK

Replay attack or Screen-in-screen attack is when the end-user takes a photo from another screen to upload a photo of an identity document or face in real time. Identifying such fraud requires highly capable systems when photos are taken from high-resolution devices.

TOO MUCH FLASH ON THE CARD

Sometimes fraudsters flash light on cards to hide information and to manipulate the system. Shufti Pro does not accept such verification attempts and disregards them. This is one of the new fraud techniques that we identified during 2021.

PUNCHED DOCUMENTS

Punched documents are not acceptable for verification under KYC laws in several countries. The punched document indicates an expired document, flagged or fake document, or invalid document, and this varies across legislation. The types of punch and their place on documents varies country wise. Shufti Pro's AI is trained with real data to identify these types of documents in seconds.

CHANGED PHOTO ON ID DOCUMENT

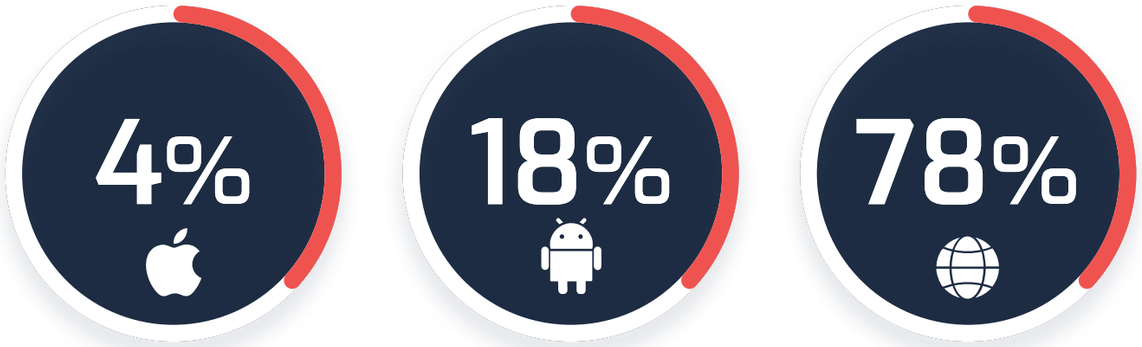
It is quite common among the fraudsters to paste a high quality colour printed photo on the ID documents to manipulate the system. Or sometimes they photoshop the face photo on the identity document that somehow matches the resolution of the photo of the entire ID document. These are some of the new techniques used by fraudsters to manipulate the IDV systems.

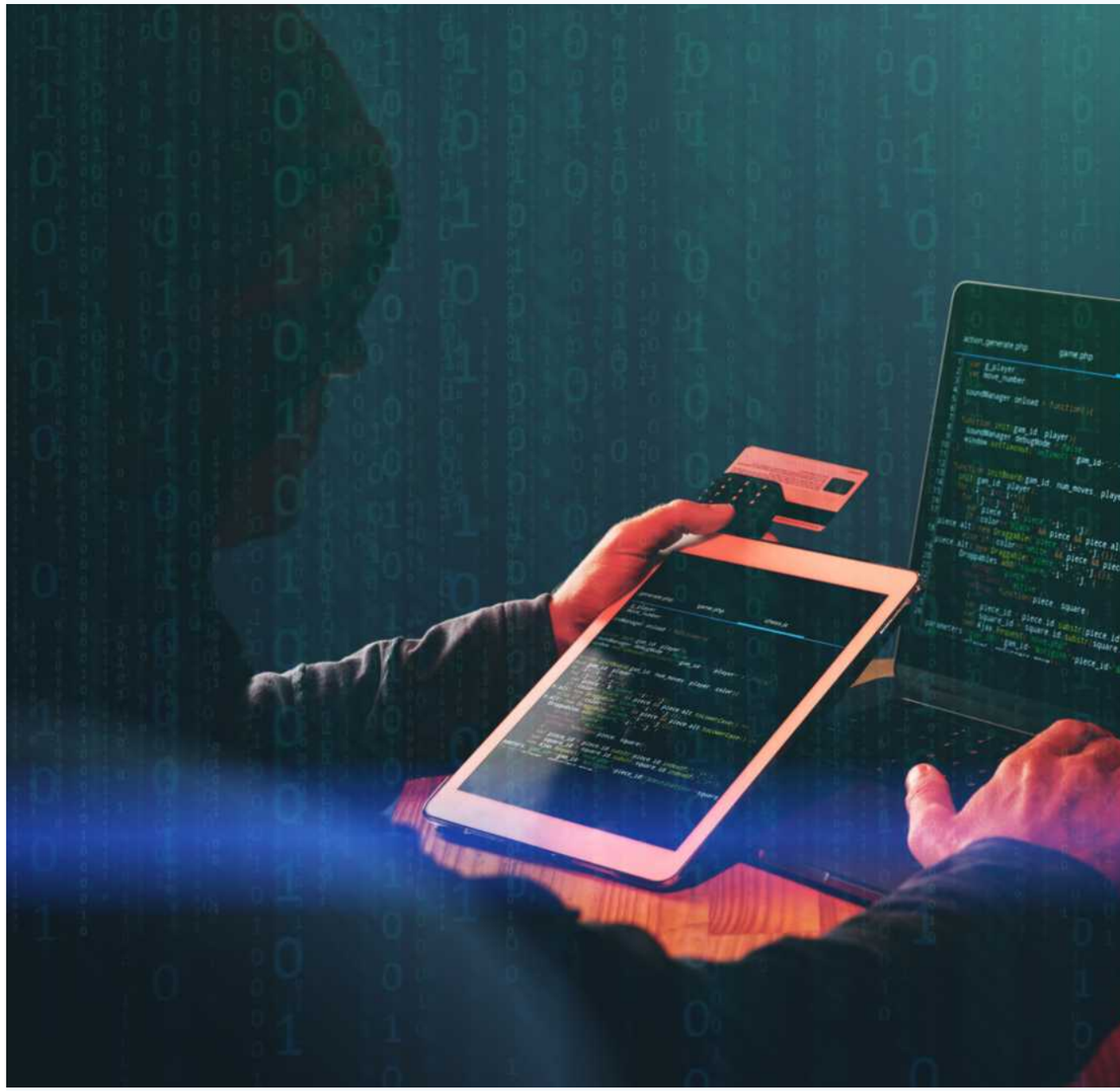
COLOURED OR BLACK AND WHITE PHOTOS

Coloured or black and white photos of the identity document are often used to dodge the system. Thanks to the AI it is captured in real-time within seconds.

DEVICES THAT ACCOUNTED FOR THE HIGHEST ID FRAUD RATE IN 2021

iOS, Android, Web - devices and operating systems have some level of vulnerability that might be one of the reasons behind the rise in identity fraud. In 2021 **78%** of the fraud attempts were made through web devices, followed by **18%** through android and **4%** through iOS devices.





ART MARKET – HOW IT FACILITATED CRIMES IN 2021

After the biggest ***Pandora Papers*** leak in October 2021, attention of all the regulatory watchdogs shifted to the art market. Some big names came to the surface for laundering money and financing terroism groups using art pieces and antiquities. The 11.9 million files exposed 35 world leaders and also shed light on the secret finances of 300+ public officials. The FATF, FinCEN and other law enforcing bodies are devising policies to regulate the art market and combat money laundering. The main target is to ensure identity checks and background screening of individuals.

On the other hand, the ***White House*** flagged the art market and declared it a safehouse for shady financial dealings on December 6, 2021. This warning was part of the WH report “Strategy on Countering Corruption”. According to the report,

“The art market is vulnerable to a range of financial crimes. Built-in opacity, lack of stable and predictable pricing, and inherent cross-border transportability of goods sold, make the market optimal for illicit value transfer, sanctions evasion, and corruption.”

Back in 2020, there was a ***global crackdown on the art and antiquities market*** by Europol, Interpol and the World Customs Organization (WCO). **103** countries were investigated and **19,000+** archaeological artefacts, ceramics, historical weapons, paintings, fossils, and other artworks were recovered. The action led to an arrest of **101** for art trafficking.

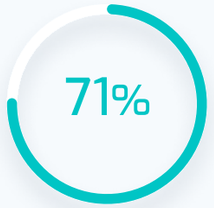
2022 PREDICTIONS THAT WILL THREATEN THE CORPORATE SECTOR

In 2021, some of the biggest ransomware attacks were reported in different industries. Businesses, in 2022, must be prepared to face the severe consequences of the social engineering attacks. This year, all the stolen data will be used in different forms to open fake e-wallet accounts and bank accounts for money mules. Let's take a look at what 2022 will look like if we talk about frauds.

2021 FRAUD PREDICTIONS THAT LEFT BUSINESSES IN SHOCK

BEC FRAUD TO INCREASE

Around 71% of the companies experience Business Email Compromise (BEC) fraud in 2021. Moreover, the remote working trend was significantly used for BEC



HEALTHCARE FRAUD WILL RISE

As we moved to the mid of 2021, fraudsters' attention shifted to healthcare institutes for their illicit gains. As predicted in 2020, criminal attempts to steal patient data increased

FRANKENSTEIN FRAUD TO CAUSE TROUBLE

Also known as synthetic identity fraud, perpetrators used all the stolen data and created new IDs for the sake of money in 2021, However, this fraud is forecasted to increase in 2022 as well

SYNTHETIC IDENTITY FRAUD TO DODGE ID VERIFICATION

As predicted by **Shahid Hanif**, the Founder and CTO of **Shufti Pro**, synthetic identity frauds showed a massive rise in 2021. After witnessing the rising fraud attempts using manipulated identity documents, **Shufti Pro**'s CTO is certain about the increase in synthetic identity fraud (frankenstein fraud) in 2022 as well. He has suggested all businesses to employ more robust measures to identify manipulated ID documents before it gets too late. Fraudsters have become strategically stronger during the pandemic and considering the level of manipulation we have encountered this year, it is nearly impossible for businesses to combat frankenstein fraud in the years ahead.

DEEP FAKE ATTACKS TO HINDER FACE VERIFICATION

Just like 2021, organisations must be prepared to face a spike in deep fake attacks, especially for hindering biometric authentication. A 2021 report from ***Cybernews*** revealed that the number of expert-crafted video deep fakes doubles every six months.

REMOTE WORKING TREND WILL BE EXPLOITED

This year, phishing emails were targeted at all the companies that supported remote working during the pandemic. The subject lines enticed organisations to reply with sensitive information about their emails. Ultimately, bad actors have all the information they need to misuse in 2022.

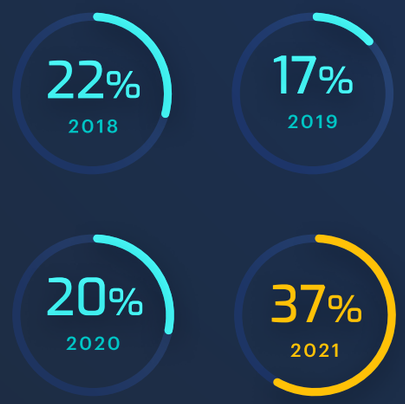
CRYPTO, NFTS, AND CBDCS TO BE THE NEW TARGET

#Cryptocurrency #NFTs were trending on Twitter the entire year and for all the right reasons. Crypto investors increased and by the end of 2021, metaverse gained hype. However, this hype and trend came at a price. Money launderers laid eyes on the massive adoption of cryptocurrencies and laundered millions through virtual assets. That's not all. The Central Bank Digital Currencies (CBDCs) also became the target of financial criminals. China was the first country to introduce CBDC at national level in 2021 and ***millions were laundered through Digital Yuan*** in November 2021. In 2022, analysts have predicted an increase in these fraudulent activities.

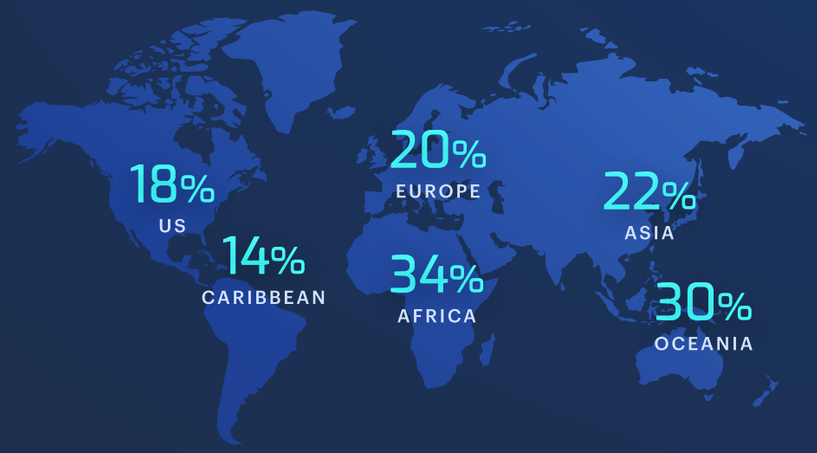
KEY TAKEAWAYS FROM 2021

The year 2021 was yet another rollercoaster year for businesses. The identity fraud and financial crime rate significantly increased and 2022 is expecting a higher rate. Just like the finance industry, the cryptocurrency industry is also the target of fraudsters. Henceforth, rigid regulations for this sector are in the pipeline. So, crypto exchanges must prepare themselves for a regulatory change next year.

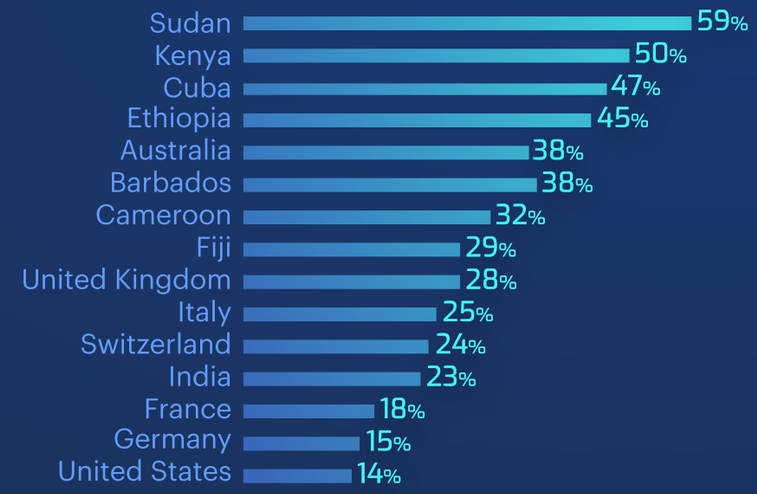
PRE-PANDEMIC AND POST-PANDEMIC FRAUD RATE



REGIONS WITH THE HIGHEST IDENTITY DOCUMENT FRAUD RATE



COUNTRIES WITH THE HIGHEST RATE OF BIOMETRIC FRAUD



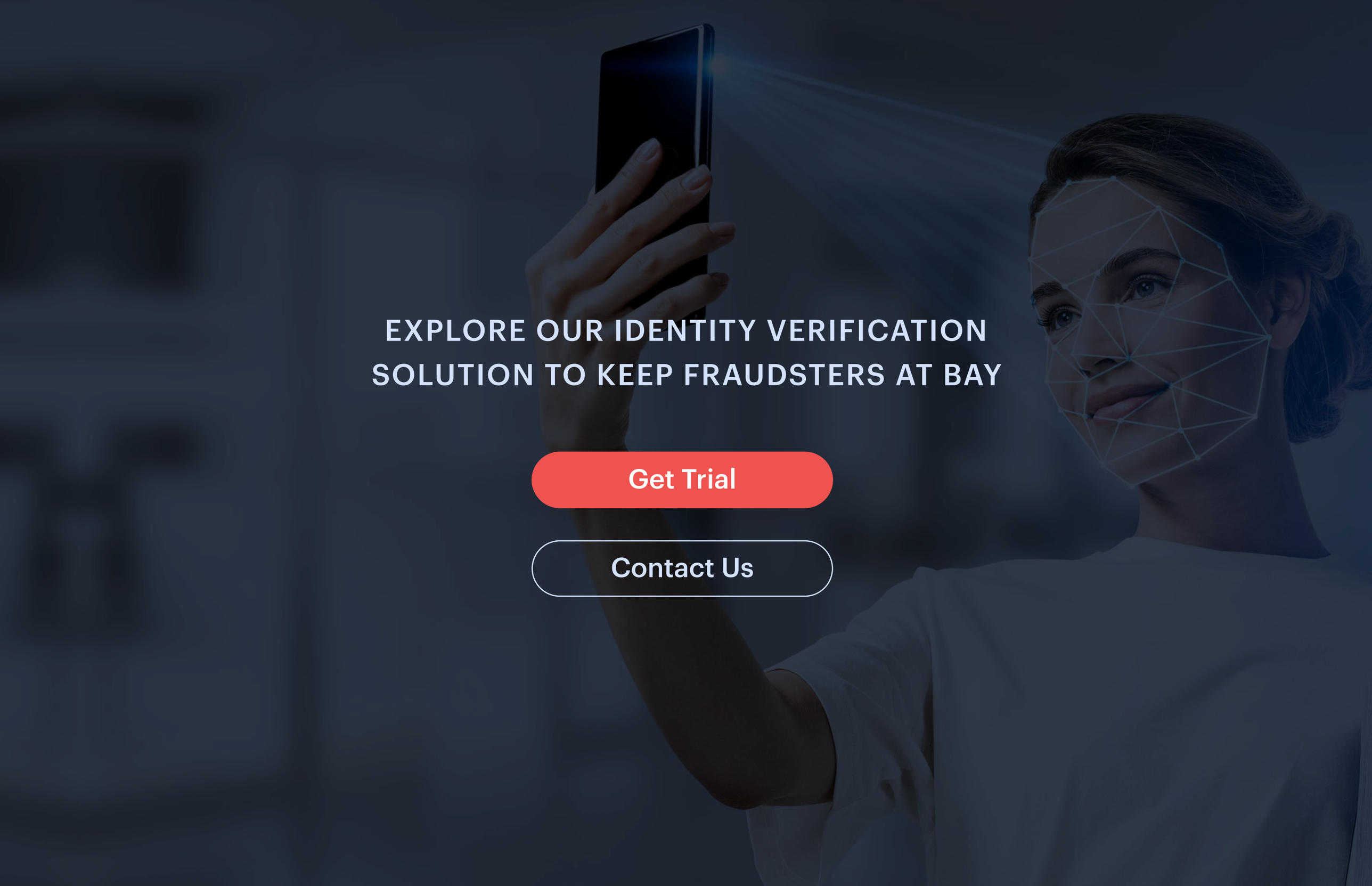
32% ID documents could not be verified for originality

19% Image on the identity document was forged

8% Face and image on the ID document couldn't be matched

What to Expect in 2022?

- Rise in deep fakes attacks
- Increase in synthetic identity fraud
- Crypto and NFT-based criminal activities
- Fraudsters will target remote working trend


EXPLORE OUR IDENTITY VERIFICATION
SOLUTION TO KEEP FRAUDSTERS AT BAY
Get Trial
Contact Us

Shufti Pro

Expanding services to 230+ countries and territories in a short period of time, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure. With enough experience in technologies like machine learning (ML), OCR, artificial intelligence, and Natural Language Processing (NLP), Shufti Pro strives to provide the best identity verification services to verify customers and businesses online.

Shufti Pro's cost-effective solutions help businesses to prevent fraud and illicit crimes that can ruin the integrity and brand reputation of your business. Our perfect solution suite consisting of KYC verification, AML screening, ID verification, Facial Recognition, Biometric Authentication, Video KYC, OCR, and KYB helps to improve your company's fraud prevention, Know your Customer (KYC) and Anti Money Laundering (AML) regulatory efforts by automating the workflow. With single API integration, Shufti Pro empowers you to verify customers with document checks from 3000+ ID templates and business entities from 200 million companies data.