Shufti Pro

Global Identity Fraud Report 2020

Content

Victor Fredung, CEO of Shufti Pro, shared his views on the rising number of fraudulent activities in 2020.

Foreword

“Cybercrimes have approximately doubled this year and we need a better approach for fighting fraud in the year ahead. Fraud evolved tremendously during 2020 and more advanced approaches to fraud prevention must be taken in order to secure your business and customers from million-dollar identity and payment fraud.

Our Fraud Report 2020 is drafted to provide you with a birds-eye view of identity fraud that we captured along with the findings that global researches reported. Find out about multiple types of spoof attacks, and document frauds to learn how they might infiltrate their business.”

Shufti Pro

“

Shahid Hanif, CTO of Shufti Pro, said that the increasing ratio of fraud demands thorough KYC and AML measures against multi-faceted fraud in 2021.

Foreword

“The pandemic, rising demand for digital services and the surge in fraud has taken businesses by surprise. Financial and identity frauds are on the rise increasing the demand for online identity verification solutions. Shufti Pro experienced a rise in demand for IDV and face verification solutions in 2020, while our intelligent KYC/AML and biometric verification solutions captured multiple ID and face spoof attacks. This report will provide you with valuable insights into the identity frauds that occurred in 2020 to help you make beneficial decisions for your business in 2021.”

Shufti Pro

Global Fraud Overview

Global losses from fraud have tripled to USD 32.39 billion in 2020 from USD 9.84 billion in 2011.[1]

1: Merchant Savvy

The Covid-19 pandemic has initiated an inevitable wave in the application of digital technologies due to the social distancing norms. Individuals and companies all over the world have ought to adopt the new techniques of work and life. The online marketplaces kept growing despite the uncertainty due to the pandemic in 2020.

We encountered a 3.36% rise in global identity fraud in 2020, as compared to 2019.

Unfortunately, a surge in fraud and identity theft trailed this tremendous growth of online businesses. It is likely that these scams and frauds will increase in intensity after the pandemic. A PWC report[2] on global fraud disclosed that 47% of companies experienced a fraud case in the past 24 years. Shufti Pro encountered a significant increase in identity fraud in 2020. Fraudsters took full advantage of the worsening condition across the world and there was a 3.36% increase in fraud.

Reports from ConsumerAffairs[3] indicated that the United States experienced the most identity frauds. According to ConsumerAffairs, 7 - 10% of the US population faces identity theft every year and 21% of them face this multiple times.

While delivering our services in 2020, around 46% of the total Egypt verifications conducted through identity documents were fraud attempts.

2: PWC Global Fraud Report 3: 2020 Identity Theft Statistics

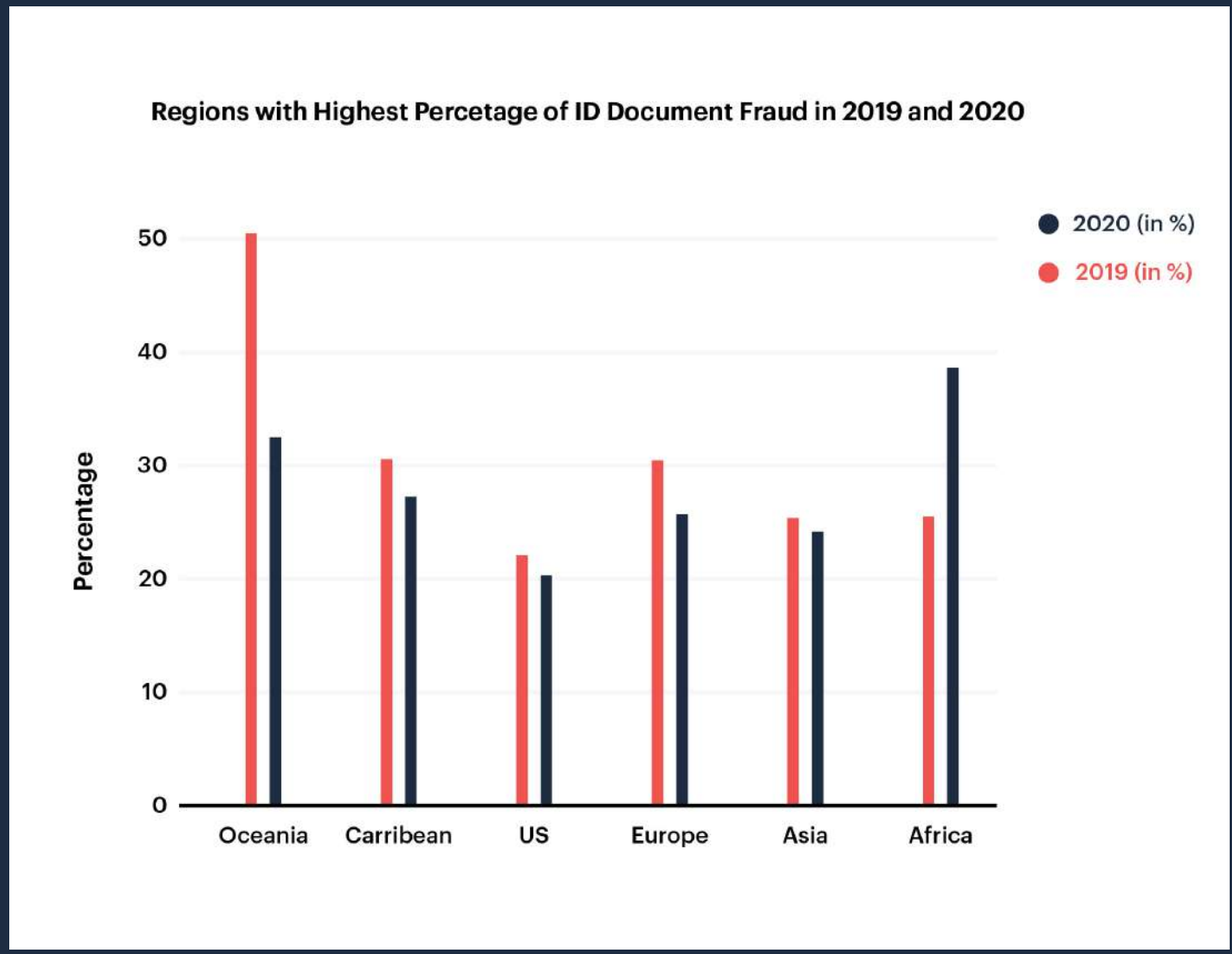
Second state where we experienced the highest rate of identity document fraud was Singapore in which 27.84% of the total identity document verifications performed were fraud attempts to surpass identity verification checks.

Next in line is Switzerland with approximately 21.36% identity document fraud captured by our AI-powered solutions. Reports from Statista have also revealed that there will be an approximately 80% increase in identity fraud by the end of Q3 of 2021[4] in the European Region.

While the number of verifications performed by Shufti Pro increased four times, the fraud became more sophisticated. In order to reduce false negatives, Shufti Pro now offers the merchants to allow up to three attempts for end-user verification.

4: Global Identity Fraud Statistics

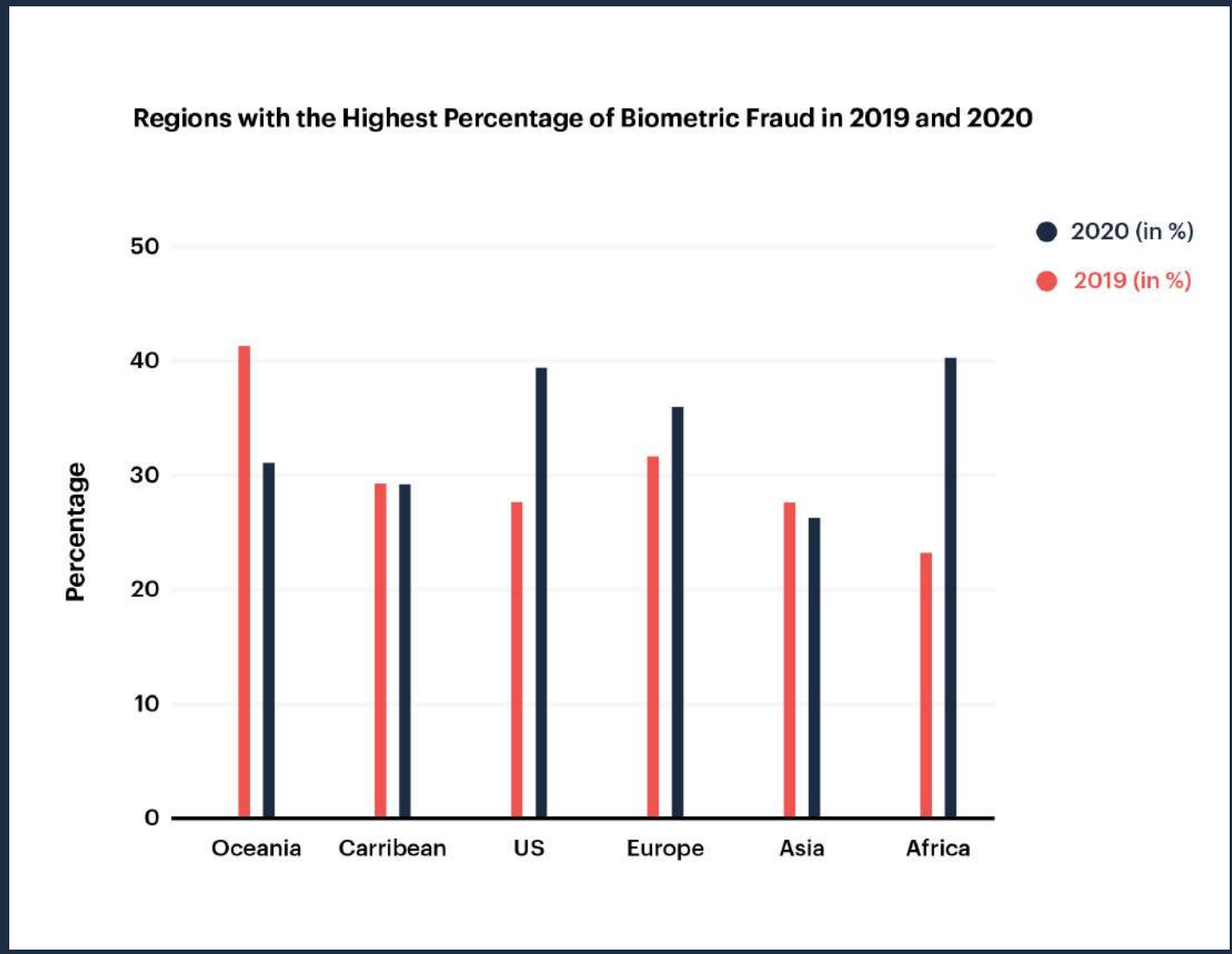
While verifying identities in different regions of the world we witnessed varying intensities and types of frauds. Here's a brief overview of regions that encountered the most frauds in 2019 and 2020.



So legitimate clients were onboarded with ease while fraudulent attempts were identified through enhanced AI-checks. Counterfeit IDs, synthetic IDs, and doctored identity documents were frequently used to manipulate the document verification checks. The use of 2D and 3D face masks along with deep fakes increased in 2020.

The surprising point here is that the total global fraud rate decreased this year. Although document and face frauds evolved technically and strategically in 2020, we experienced an overall decrease in fraud rate. But the fraud trends were unique in different countries/ regions and at different periods during the year 2020. An increasing number of clients started using biometric authentication in combination with document checks to enhance their security.

We witnessed varying intensities and types of biometric spoof attacks. Here's a brief overview of biometric spoof attacks that we encountered in different regions 2019 and 2020.



Criminals have developed sophisticated methods of messing with identity documents. However, they haven’t been lucky with biometric frauds. Which signals the rising significance of biometrics for fraud detection in coming years. Read the report to find the different types of methods that criminals use to manipulate identities and how AI-based IDV solutions capture them. Get valuable insights on 2020 fraud trends of different regions and 2021 fraud predictions plan a risk-free year ahead for your business.

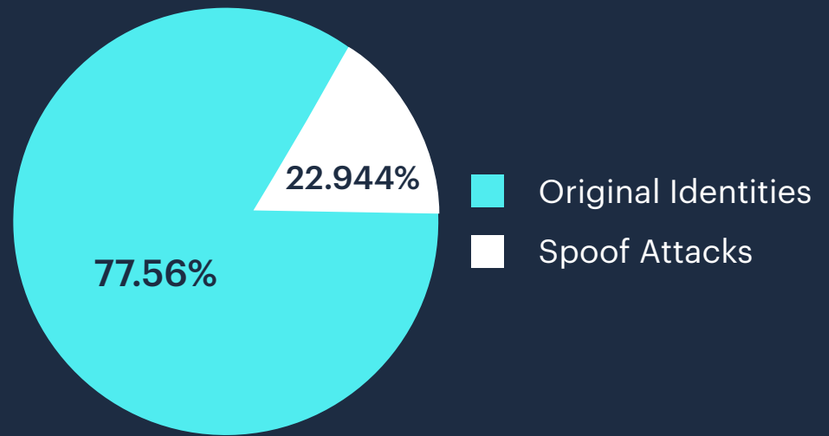
Biometric Fraud

Global biometric fraud rates dropped dramatically in 2020, but varying trends were witnessed in different regions. The fraud became sophisticated which increased the demand for advanced biometric solutions. This section will elaborate different types of spoof attacks that we identified through our face verification technology.

Biometric frauds are still not sophisticated enough to beat biometric authentication checks. However, we were surprised to see a significant evolution of biometric fraud in 2020. 2D and 3D masks, photoshopped images, and deepfakes were the most used methods to dodge biometric authentication.

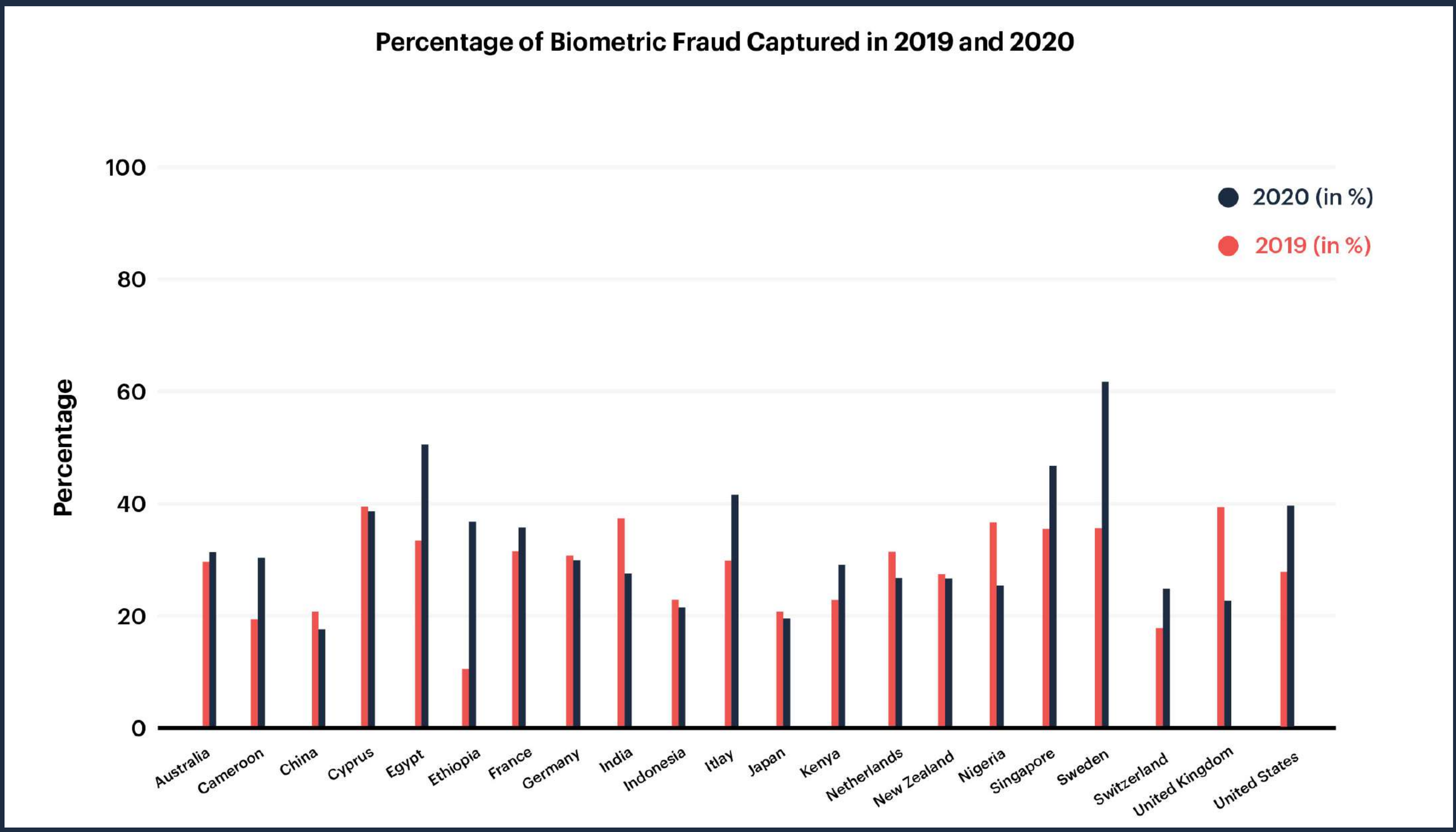
While we were performing face verification checks, we encountered more sophisticated facial spoof attacks as compared to 2019.

In 2020, Australia, Cyprus, Egypt, USA and Italy experienced skyrocketing increase in biometric frauds. On the contrary, biometric fraud in China, India, and UK decreased.



Out of all the face verifications performed, over 22.44% were biometric fraud attempts in 2020.

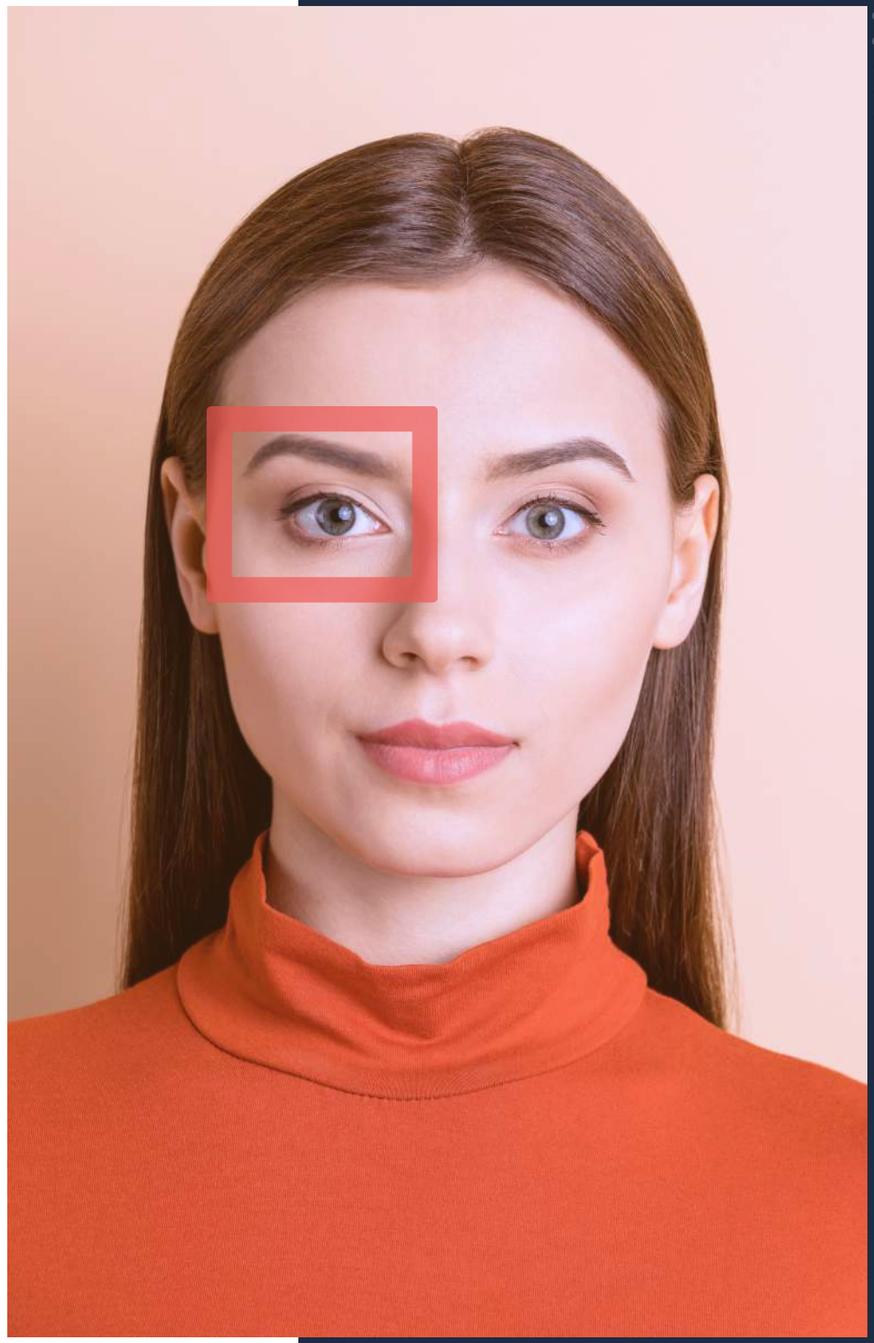
Although the overall fraud rate has decreased, biometric fraud attempts in Australia, Bahamas, France, Italy, and some other countries have increased in 2020.



Photoshopped Images

Photoshopped images are the intentionally modified or reconstructed digital images. The edits are sometimes so minimal to identify with naked eye. Eye colour, face symmetry, hair colour, skin tone and even the shape of face can be edited through photoshopping. Photoshopped images are also utilised by fraudsters for carrying out monetary crimes, malicious attacks, disseminating incorrect information, and accessing user identity.

During 2020, we encountered a rise in biometric fraud in European region, the USA and Africa. On the other hand, there was a surprising decrease in biometric fraud in Oceania, Carribean and Asia.



In the latest survey[5], the scientists discovered that most of the malicious photo editing is done using widely available tools, any user can distort particular areas of a face to completely change an individual's expression, such as turning joy into sorrow or a clear gaze into the expression of an insane individual. Fraudsters edit the hair color, skin tones, eye color and other minor facial attributes to surpass the biometric checks. Identifying these checks with naked eye is near to impossible. This is when artificial intelligence comes into action. AI collects all facial features from a photo and compares them with the face in the record, if there is even a minute edit made through photoshopping, it is identified within seconds.

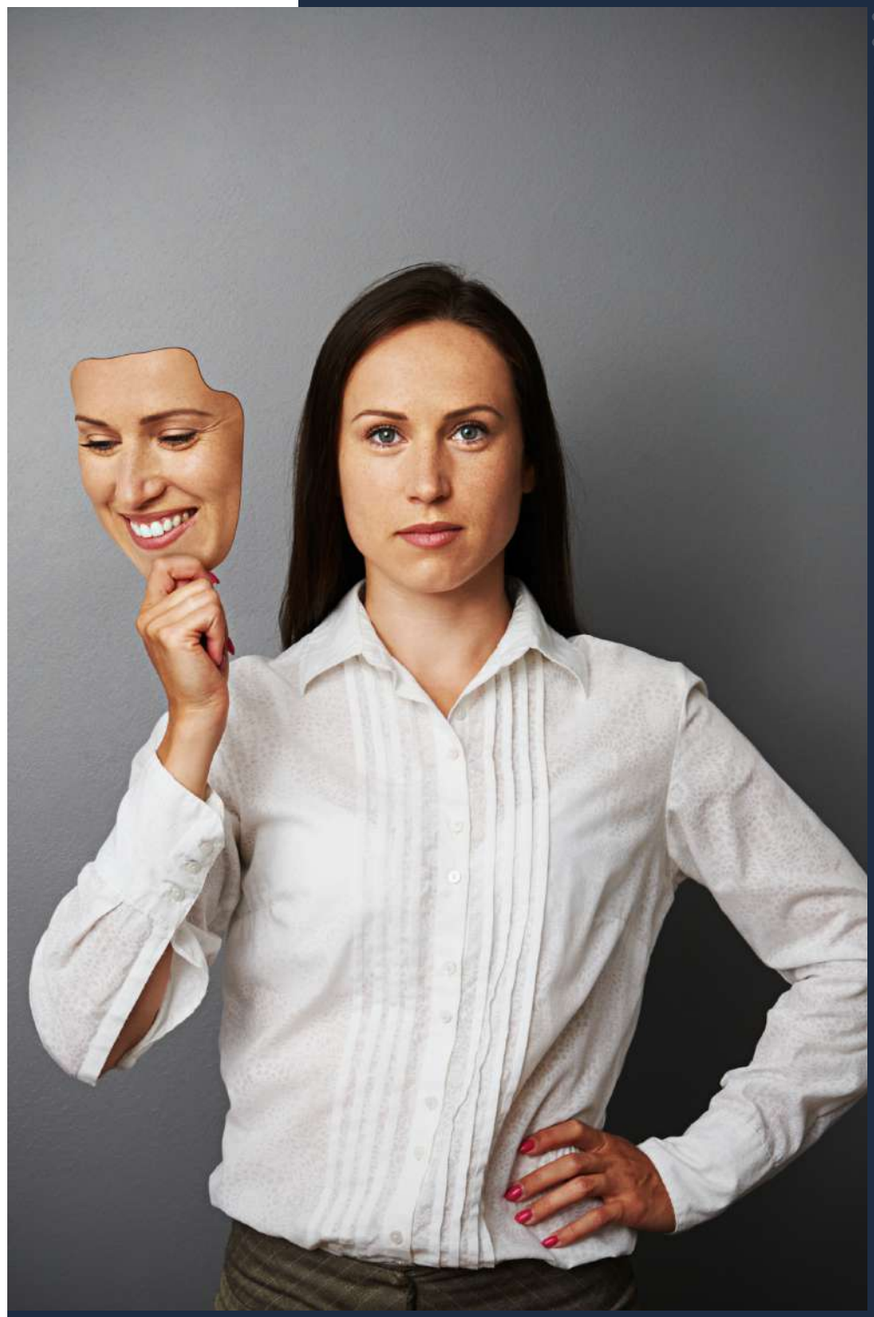
AI-based biometric verification solution of Shufti Pro performs face verification checks to identify photoshopped images. The AI is trained with multiple photoshopped and original images to enhance its accuracy. It identifies minor photo tweaks and captures fraud in the blink of an eye.

Synthetic identities (discussed later in this report) developed by combining the photoshopped photos of people and stolen identity documents are commonly used to pass the IDV checks. Fraudsters pick the images of victims from social media, photoshop them and use them with stolen identity documents to surpass the identity checks. If the merchant is only verifying the identity documents, the chances are high that the fraudsters might get past the checks. So we always recommend our clients to use biometric authentication along with face verification.

5: Artificial Intelligence

2D and 3D face masks

2D and 3D masks are one of the most sophisticated methods used to surpass facial biometric technology. The presentation attacks are intended to reverse the face verification system by performing a facial artefact. Traditional face artefacts incorporate printed pictures, replaying the video, 2D and 3D facial masks.



Imposters utilise advanced printing automation to formulate a 2D mask and sometimes purchase a 3D mask online for a few hundred bucks. Sometimes the end-user cuts out eye holes on a paper-backed photo to manipulate the face verification solutions through eye movement.

In 2020, we experienced more sophistication in 2D and 3D face masks as compared to 2019. However, fraudsters could not surpass face verification checks.

Failed liveness detection

With the advancement in biometric technology, attacks on conventional identity verification solutions have become more and more intelligent. The problem is that fraudsters use images of paper-backed photos or pick random photos from the internet to manipulate the system. Picking images from the internet or social media is quite easy these days. The imposters utilizes these images to get past the biometric check.

By using 3D mapping, Shufti Pro detects the 3D angles and minor facial movements to ensure the presence of a real person. It ensures to check for relevant markers for liveness detection. Those relative markers consist of checks for eyes, skin texture, photoshop, age and hair colour differences.

Its deep machine learning algorithm makes sure optimal micro expression analysis is conducted through adequate data comparison. Referring to a computational algorithm, various points on the picture are matched to that of a previously digitized template. Shufti Pro's liveness detection shows an individual's live presence and prevents facial spoof attacks as well.

The majority of biometric fraud attempts captured in 2020 were 2D and 3D spoof attempts. The end-user either displayed a paper-backed photo or took a photo from the screen of another device.

Deep fakes

Deepfakes refer to videos that have been edited by utilising deep learning so that people believe the false. For instance, videos with changed background or faces swapped in the video. Sometimes, fraudsters edit certain words or statements in the videos to make them more authentic.

Deep fakes are computer vision techniques to deceive the face verification checks. By 2022, they say, that estimate will be higher like 720,000 – and anyone is unsafe[6]. All that is needed is a photo, video or audiotape of the innocent. Deep fakes were generated to create an imitation of someone from a comic prospect.

6: Deepfake

This technology has been applied in many 3D films for popular characters. Today, fraudsters use deep fake to create a fake video to dodge liveness detection checks. Such videos are compilation of images of a victim that are incorporated in such a manner that it seems true. Deep fakes were generated to create an imitation of someone from a comic prospect. This technology has been applied in many 3D films for popular characters. Liveness detection and anti-spoofing checks ask the user to blink, smile, turn/nod, make random faces, speak random numbers, etc. These measures help in mitigating the risk of these emerging threats.

It is predicted that 180,000 deep fake videos of victims will be online in 2021.

Fraudsters have developed sophisticated ways of fooling biometrics and every attempt has a different intensity. However, AI-powered face verification checks can identify these attempts in seconds.

Fraud	Intensity of fraud	Face verification checks to detect fraud
Photoshopped Images	Medium	Anti-spoofing measures
Failed liveness detection	High	Facial recognition, 3D depth perception
Deep fakes	High	Liveness detection, depth mapping
2D and 3D face masks	High	Textual analysis, depth mapping

Biometric Fraud Rate by Countries and Territories

Shufti Pro is a global identity verification service provider. Among the 230 countries and territories we serve, take a look at the countries with the highest ratio of biometric fraud between 2018 and 2020.

Biometric Fraud Rate by Countries and Territories Between 2019 and 2020		
COUNTRIES	**2019 (in %)**	**2020 (in %)**
Australia	29.39	31.27
Cameroon	19.61	31.51
China	20.50	17.37
Cyprus	39.29	38.04
Egypt	33.33	50.04
Ethiopia	10.01	36.36
France	31.37	35.61
Germany	30.75	29.40
India	36.97	27.24
Indonesia	22.30	21.13
Switzerland	17.75	24.12
Italy	29.79	41.14
Japan	20.90	19.33
Kenya	22.70	26.77
Netherlands	31.52	26.54
New Zealand	27.19	26.37
Nigeria	36.90	25.44
Singapore	37.58	46.43
Sweden	35.71	61.54
Switzerland	17.75	24.14
United Kingdom	39.28	22.16
United States	27.84	39.33

Document Fraud Types

Different regions of the world experienced varying rates of ID document frauds in 2020. Although the overall fraud rate decreased, the rate was high in some regions by document type. Moreover, the intensity of identity document frauds was higher than what we had expected.

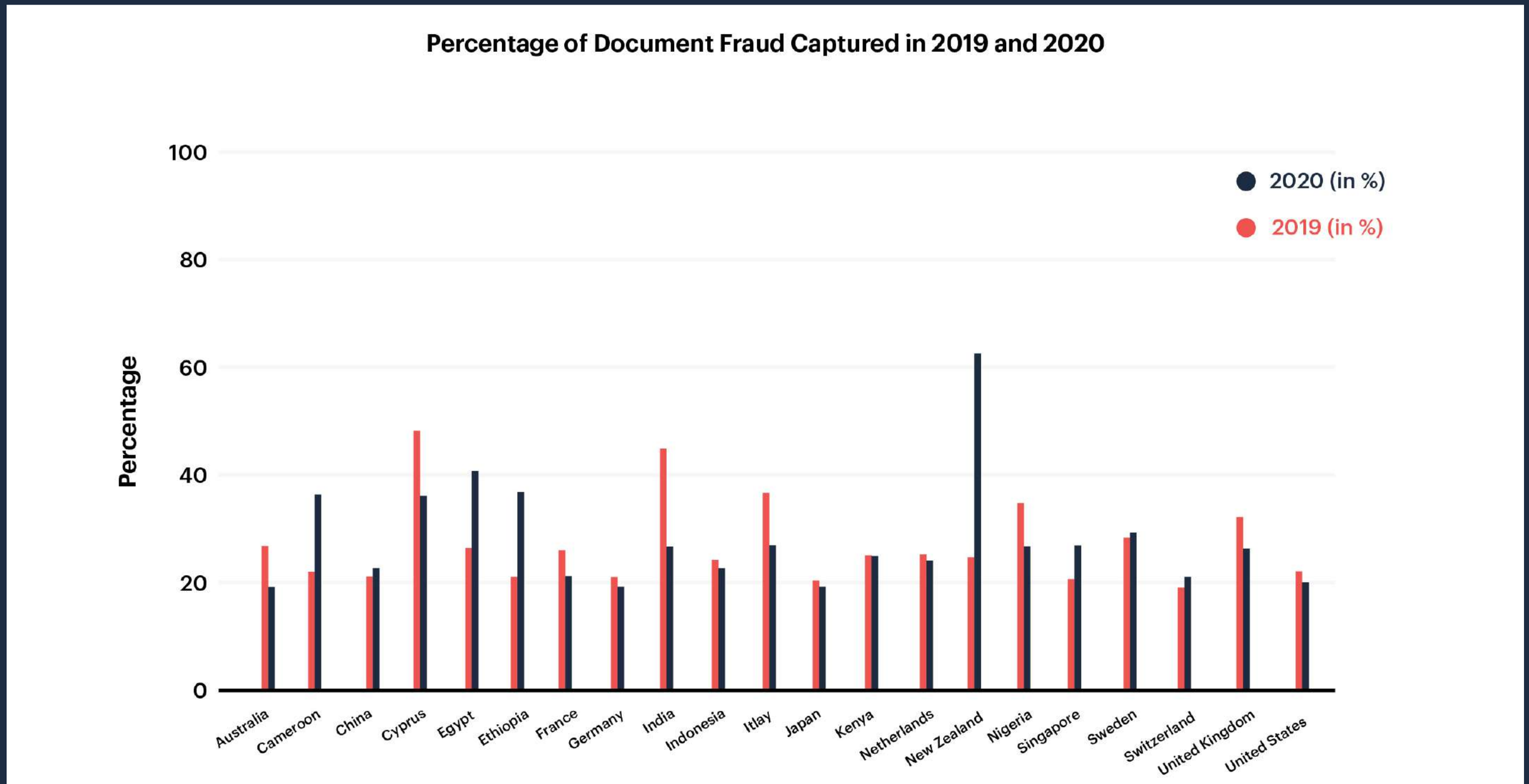
Fraudsters not only use 2D and 3D masks for deceiving identity verification checks, but using false or stolen identity documents is more common these days. Tampering with identity documents and creating fake identity documents are two of the most common strategies that criminals use to surpass identity verification checks.

In 2020, there was a significant increase in identity document fraud in different countries of the world. China, Egypt, Switzerland, and Sweden showed the most increase in fraud. On the other hand, the Australia, the UK, Cyprus, and Germany had a slight decrease.

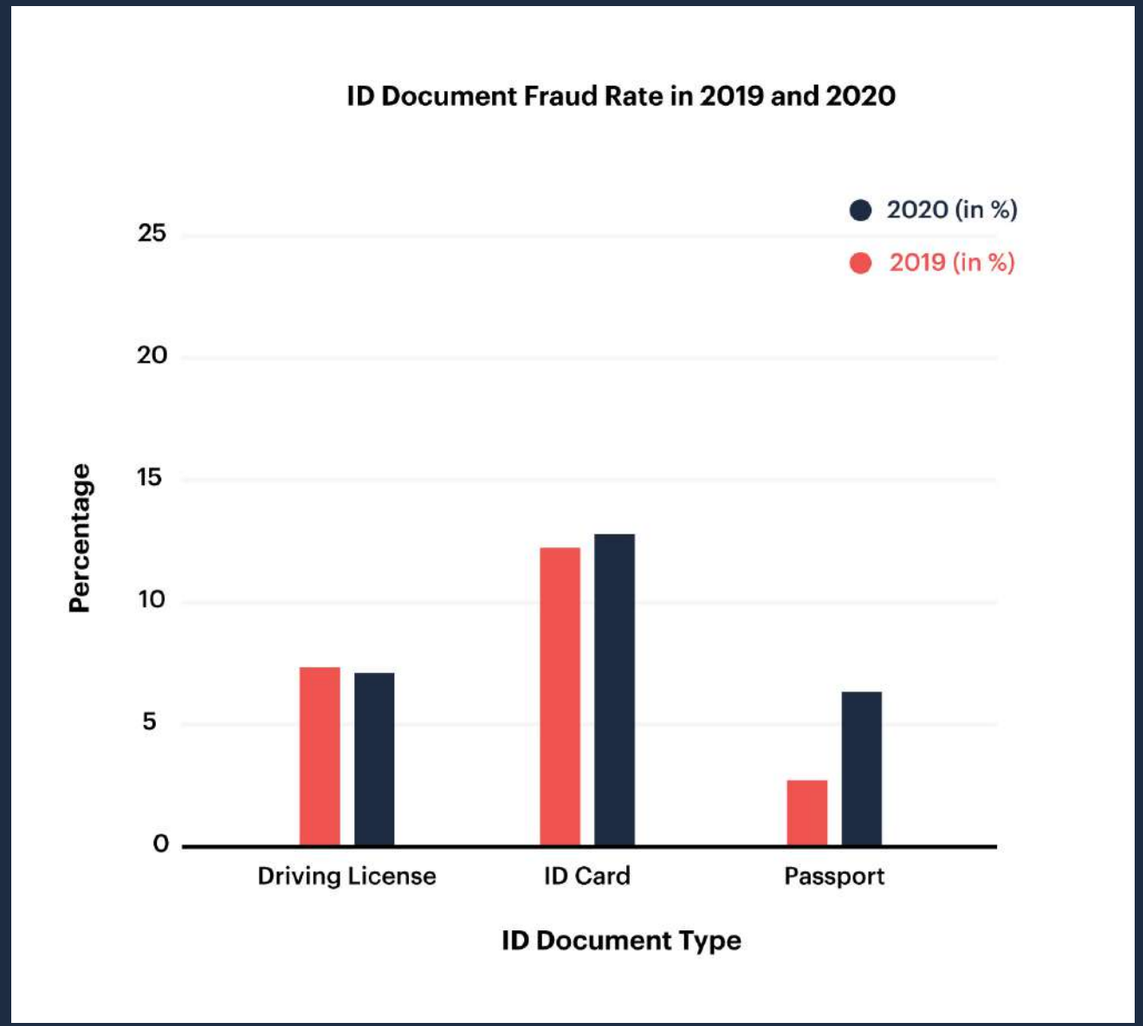
As per our document verification record, more than 19.78% of document verifications that we performed in 2020 included some sort of document fraud attempt. There was 1.34% increase in document fraud in 2020 as compared to 2019.

This part of the report will elaborate the types of document fraud that we captured globally. Passports, ID cards and Driving Licenses were used to bypass the document checks. Continue reading to know about fraud trends in different regions.

Between 2019 and 2020, all types of identity documents were extensively used for attempting fraud and forged ID cards were used majority of the times. In 2020, 12.96% of the ID document fraud attempts were made using by ID cards.



The document fraud takes unique forms when initiated through different identity documents. Although the intensity of fraud was low in 2020 the diversity remained intact, as ID cards were used primarily to manipulate the IDV checks.



Synthetic Identity Fraud

Synthetic identity fraud is when fraudsters consolidate both genuine and false data to generate a new identity. Imposters may generate synthetic identity using conceivable authentic SSN with inaccurate PII (Personally Identifiable Information). Synthetic identity fraud is difficult to capture without an in-depth screening of an identity document and multi-factor authentication of an identity.

We experienced a significant increase in synthetic identity fraud while performing document verification checks.

According to the Federal Reserve Report[7], synthetic identity fraud is the hardest fraud to detect due to which 85 to 95% of this fraud is not flagged during identity verification.

7: Federal Reserve Report

There are numerous methods of synthetic identity fraud, out of which the following three methods are extensively used:

Identity fabrication - An entirely new identity is created that does not have any Personally Identifiable Information (PII).

Identity manipulation - In the identity manipulation method, fraudsters modify PII and create a new identity. For example, a fraudster changes the name and date of birth of an ID card keeping other information the same.

Identity compilation - This method involves a combination of fake and real identities for creating a new identity. For instance, some part of the PII is real, whereas the remaining part consists of fake numbers.

In any of the aforementioned methods, the primary objective of fraudsters is the same - using the new identities for other illegal activities like money laundering ,account takeover, and illegal accumulation of funds.

Fake Documents

Using artificial intelligence models for creating fake identity documents is now very common. According to our findings, the majority of these fake documents were created using stolen identities. Moreover, fraudsters submitted new identity documents for fake identities. Identities of the deceased and children are used to create fake documents. With the help of Artificial Intelligence, it got easier to design government-issued identity documents.

19.78% of document verifications failed because fake, doctored, stolen or synthetic identity documents were submitted during the identity verification process.

Fake IDs emerged in the 1970s in the US and were used to enter nightclubs and other restricted places. Today, the same strategy has become more sophisticated and used to surpass identity verification checks during the customer onboarding process. Technology has made it convenient for criminals to create government-issued ID documents. However, enhanced AI-powered document verification authenticates not just the document type, but the guilloche or rainbow prints and holograms as well. Even the slightest discrepancy in a document results in declined verification. This means your business can easily identify fraudsters and make sure they are not onboarded in the future as well. All you need is Shufti Pro's KYC solution.

Doctored IDs

By changing a small amount of information within a document, criminals create multiple versions of stolen identities. These stolen identities come from phishing attacks and data breaches primarily. For instance, changing the picture or date of birth in a stolen ID card will result in a doctored ID.

Stealing identities is no longer a problem and to ensure that regulatory authorities stay away from fraudsters, they tamper with the documents. Minor edits and minimal alterations like changing the name or using photoshopped images in the document suffice for their needs. Identifying these minor changes is quite easy with AI that is fed with sufficient real ID documents.

In 2020, approximately 13% of the document fraud was committed through ID cards.

Counterfeit or Stolen IDs

While every organisation moved to digital means, we were also expecting digital counterfeit to strike us hard. However, we experienced a significant rise in counterfeit documents. Counterfeit documents cause havoc for companies and industries since these are copies of original documents. Today, counterfeit documents also seem as original as possible which makes it harder for businesses to verify authenticity. National ID cards, passports, Social Security Cards, driver's licenses, and green cards can be counterfeit as well.

With the help of document verification, you can not only verify the information on the document but the authenticity of the document as well.

According to our reports, there was a 3.36% increase in passport fraud in 2020.

Our IDV checks are designed to identify even the minor edits in the identity documents. The AI is fed with sufficient real data and thousands of AI models are developed to cater to multiple types identity documents used around the globe. This helps us capture diverse fraud with equally diverse document checks.

Fraud	Intensity of fraud	Document verification checks to detect fraud
Synthetic Identity Fraud	High	OVI checks, miroprint scans
Fake Documents	Low	Hologram and rainbow print verification
Doctored IDs	Medium	Tampering checks, MRZ code checks, information verification
Counterfeit Documents	High	Face matching, document number verification, MRZ code verification

ID Document Fraud Rate By Countries and Territories

Different countries and territories experienced ups and downs in the ID document fraud rates since 2018. From doctored IDs to synthetic identity fraud, we encountered varying intensities of fraud in each country. Shufti Pro is a global identity verification service provider. Here are the countries and territories that faced tremendous ups and downs in identity document frauds between 2018 and 2020.

ID Document Fraud Rate By Countries and Territories Between 2019 and 2020		
COUNTRIES	2019 (in %)	2020 (in %)
Australia	27.68	19.65
Cameroon	22.06	36.97
China	21.68	23.39
Cyprus	48.22	36.18
Egypt	26.82	40.99
Ethiopia	21.43	37.04
France	26.09	21.06
Germany	21.16	19.41
India	45.14	26.84
Indonesia	24.57	23.28
Italy	37.58	27.32
Japan	20.93	19.42
Kenya	25.42	25.41
Netherlands	25.73	24.83
New Zealand	25.15	63.61
Nigeria	35.03	27.23
Singapore	20.68	27.84
Sweden	28.42	29.92
Switzerland	19.03	21.36
United Kingdom	32.59	26.46
United States	22.33	20.37

Original Document

Synthetic ID card

Missing security feature

Doctored ID card

Invalid ID card

Pixel tempering

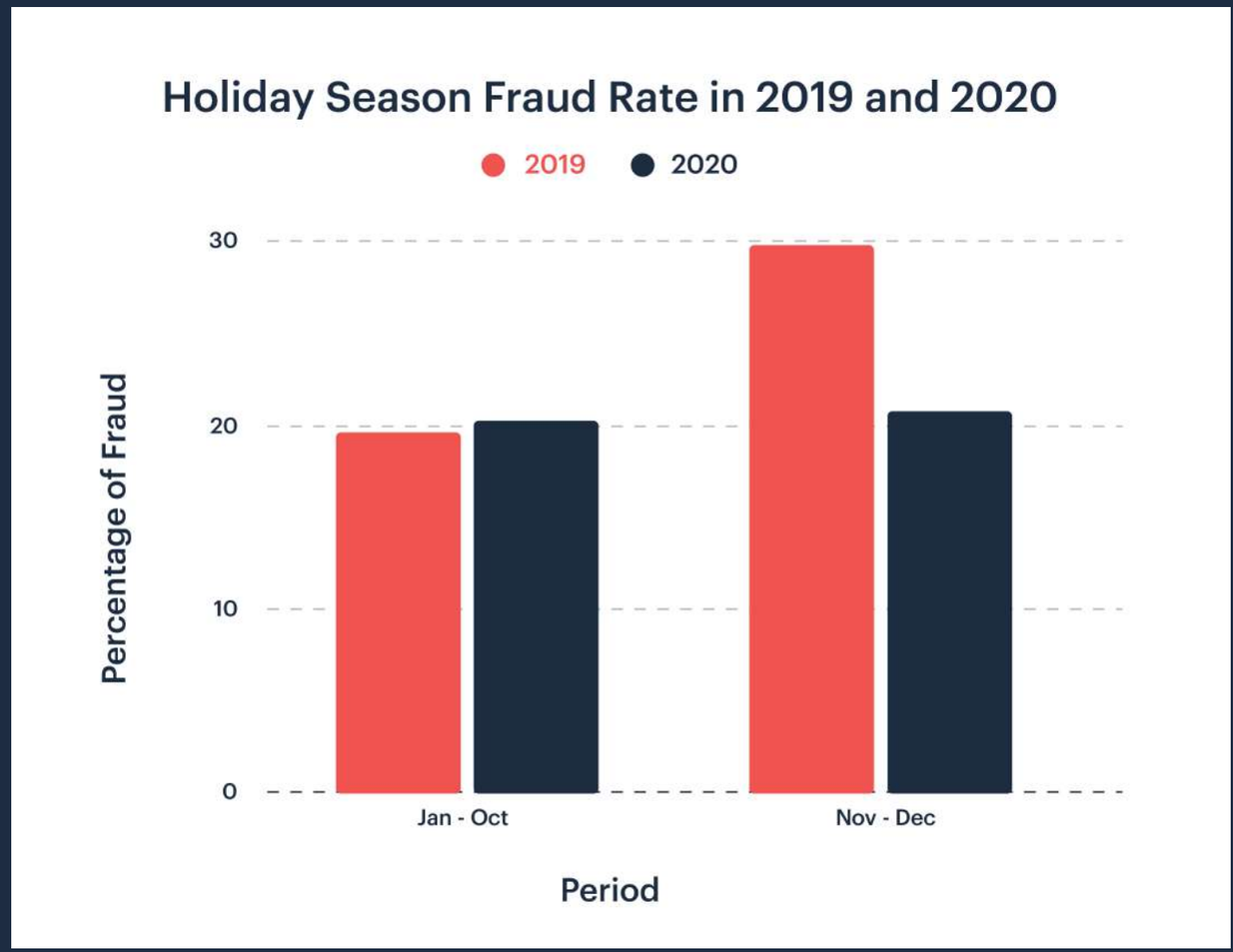
Shufti Pro

Rise in Identity Frauds During Holiday Season

2020 was the most challenging year for all businesses as sales significantly decreased and fraudulent activities remarkably increased.

The most awaited time of the year, unfortunately, faces the most fraudulent activities than anyone could imagine. In 2020, the coronavirus pandemic fanned the flame and identity fraud between November and December 2020 rapidly increased. Due to the rising number of online shoppers, fraudsters found e-commerce and other digital means a goldmine for their illicit activities.

The surprising point is, the number of fraud attempts made throughout the year is equivalent to the fraudulent activities in November and December. No matter how low the fraud rate was in 2020, the percentage of fraud during holiday season was remarkably high. Here is a summary of frauds that we encountered this holiday season and the rate of criminal activities during the rest of the year.



Industry leaders repeatedly warned all the businesses and consumers about the increase in fraudulent activities. The Federal Bureau of Investigation (FBI)[8] said that New Mexican shoppers are at risk of scams. According to FBI, these scams range from phishing attacks to identity theft and shipping scams.

The US Attorney General[9] also warned the residents about the rising number of identity theft in 2020. According to the FTC reports, about 650,000 citizens' identities were compromised since 2019 due to identity theft. The FBI warned about the fraudulent use of these identities in the festive season.

8: FBI 9: US Attorney General

The fraud rate during 2020 from January to October was 16.63% - while it was 20.55% solely in the holiday season (November - December).

Better Business Bureau (BBB)[10] also warned about the rise in holiday season scams. According to BBB, "Scams during holiday season increase and given the rapid digitisation during the pandemic, the threat for holiday season scams will significantly increase." The BBB also shared some red flags regarding the scams in online shopping.

The numbers from Shufti Pro's reports have made it clear that businesses and customers must have taken extra security measures to prevent scams and frauds.

Holiday Fraud Rate Comparison 2019-2020

Biometric Fraud During Holiday Season		
	January - October (in %)	November - December (in %)
2019	13.14	30.93
2020	22.25	23.01

ID Document Fraud During Holiday Season		
	January - October (in %)	November - December (in %)
2019	17.24	26.91
2020	19.76	19.82

10: BBB Warns About Holiday Season Scams

The Los Angeles City Attorney[11] warned the residents about the gift exchange scheme called “Letter from Santa.” He said that the letter promises handwritten notes from Santa in exchange for money and unfortunately, the majority of people fall prey to this scam. Fraudsters also send emails containing the “Letter from Santa in $19.99” subject line. The attorney warned the people to not click on any unsolicited email at any cost.

During the holiday season, the criminal entities are more active as compared to the whole year. The frequency and intensity of fraud was higher during November and December 2020. The fraud rates encountered during biometric verifications and document verifications increased in the last two months of the year. It is due to the rise in use of online shopping during 2020. An increasing number of people shifted to online shopping for secure Christmas in thanksgiving celebrations.

11: LA Attorney Warns People About "Letter from Santa Scam" during Holiday Season

Industry Fraud

Industries with the Highest Ratio of Frauds in 2020

Finance Sector

Between 2010 and 2019, the losses in online banking in the United Kingdom have increased from GBP 66.7 to GBP 111.8 million, Statista.[12]

Financial institutions are the finest target of criminals. Money laundering, identity theft, and account takeover fraud are on the rise in the financial sector. **Account takeover was up 72 per cent in 2019 with banks being the primary target of fraudsters**. In the last two to three years, the trend of money mules increased significantly as well. According to the Dedicated Card and Payment Crime Unit (DCPCU)[13], more than 1,600 social media accounts are identified that were linked to fraudulent activities. Approximately 500 of these accounts were used for recruiting young people as money mules.

Identity theft grew by 13 percent between 2019 and 2020 in the finance sector.

12: Statista 13: DCPCU

Insurance Industry

According to the Insurance Fraud Bureau[14], there is a five per cent increase in insurance fraud claims in 2020.

The insurance sector was not safe from fraudsters either, and there was a significant increase in false insurance claims. Criminals use stolen identities to claim health insurance, life insurance, and others to enjoy illegitimate benefits. These fraudulent claims cost millions of dollars to the insurance sector and rip individuals off their hard-earned benefits. Due to this, regulatory authorities such as the Reserve Bank of India (RBI) are allowing video KYC to help financial institutions fight fraud and serve customers remotely. Reports from Statista stated that 88 per cent of the insurance claims filed between 2017 and 2019 in the United Kingdom were fraud claims and accounted for significant financial loss.

According to BBC[15] UK, benefits officials fear that approximately £1.5 billion might have been lost in false claims for Universal Credit in the second quarter of 2020.

14: Fraud Bureau 15: BBC

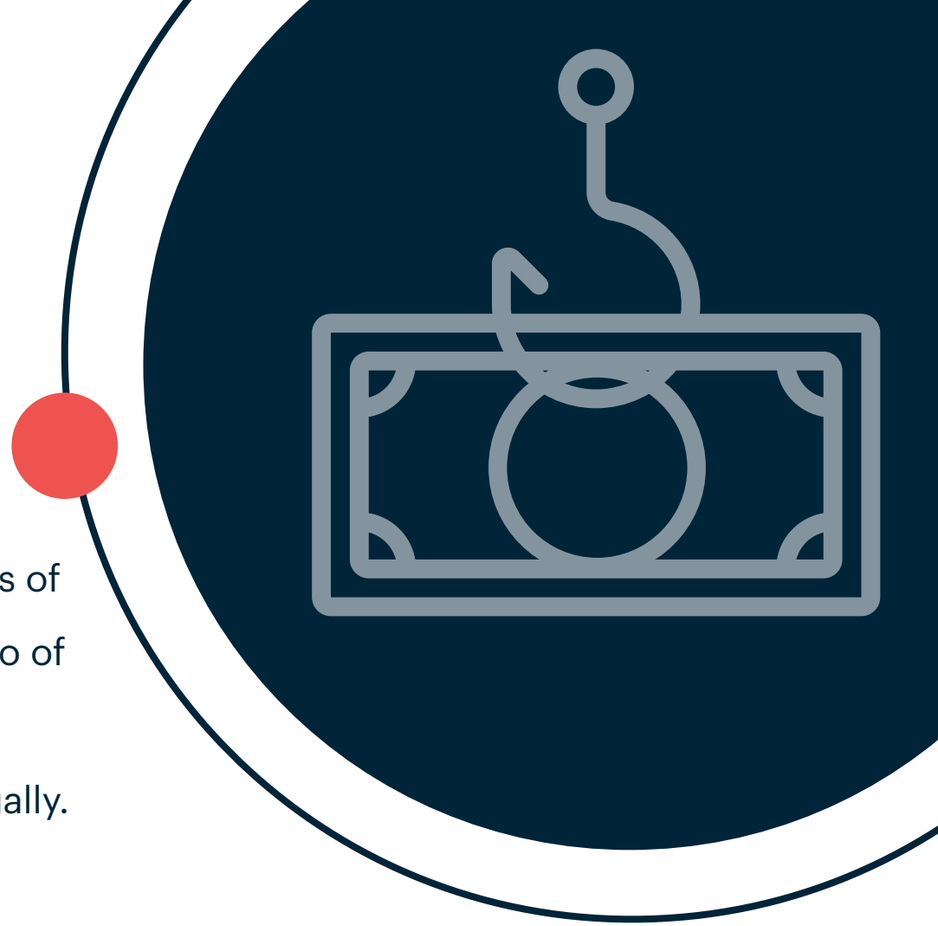
Government Agencies

According to the Annual Fraud Indicator[16], the fraud losses in the United Kingdom are estimated around £190 billion out of which the public sector loses £140 billion every year.

Unfortunately, the government organizations experienced a rise in fraudulent activities and the majority of them were unemployment insurance claims. Not just unemployment insurance, but criminals targeted the old age benefits as well. Pension fund fraud increased significantly in 2020.

16: Annual Fraud Indicator

Pension Fund Fraud



Reports from FCA and The Pensions Regulator[17] reveal that a total of £30,857,329 has been lost since 2017 according to complaints filed with Action Fraud.

A pension fund fraud occurs when an employee fraudulently acquires the pension funds of the retiree. Due to lack of employee verification systems in the corporate world, the ratio of pension fund fraud significantly increased. The coronavirus pandemic brought many challenges to life and fraudsters targeted pension funds to obtain pension benefits illegally.

Unemployment Fraud

The Employment Development Department (EDD)[18] in California experienced illegal claims fraud in 2020 due to lack of authentication checks for employee verification. Due to the pandemic, everyone faced challenges and fraudsters took complete advantage of the situation. They used fake and stolen identities of the deceased to claim unemployment insurance.

17: The Pension Regulator 18: Employment Development Department (EDD)

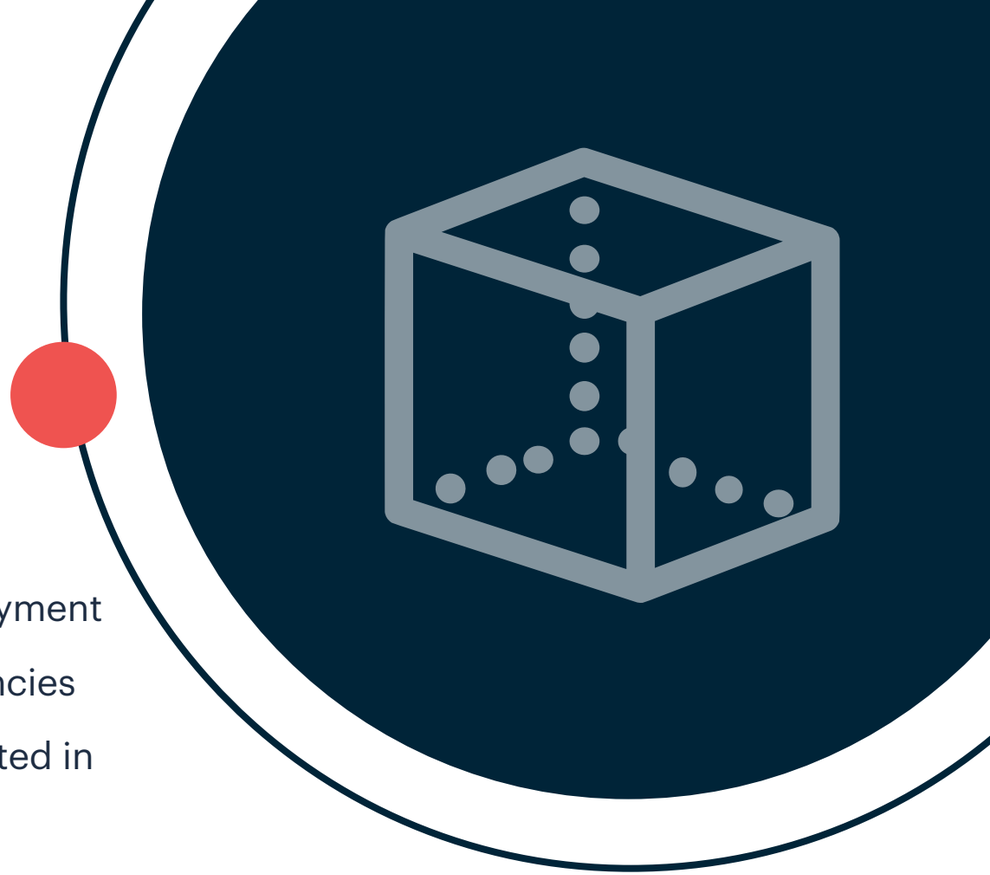
Online Gaming Industry

The number of gamers worldwide is projected to rise from 1.82 billion in 2014 to 2.7 billion by 2021, according to Statista.[19]

This year, global lockdown negatively impacted the gaming sector. The online gaming industry faced a boom in fraudulent activities, while the elderly and minors were the primary targets of fraudsters. Stolen identities, forged documents, minor exploitation, and money laundering became troublesome for the majority of the gaming platforms.

The most experienced fraud in the gaming sector was account takeover (ATO)[20] in 2020. Fraudsters steal information of legitimate players and use it to make payments and perpetrate other scams. This information can be used for phishing attacks as well. Fraudsters targeted players on online gaming platforms and used their information for credit card fraud.

19: Online Gaming Report 20: Account Takeover Fraud Report



Cryptocurrency

The crypto market is experiencing innovation to the fullest. PayPal announced its payment wallet for crypto transactions and many countries are now considering digital currencies for a better digital payment system in the future. Nevertheless, crypto crimes escalated in 2020 which facilitated money laundering.

Reports from Cipher Trace[21] estimated that crypto crimes accounted for USD 1.36 billion and 2020 experienced the highest rate of crypto crimes in 2020. Due to anonymity of crypto transactions, it gets easier for fraudsters to launder money. However, 6AMLD[22] and FATF's new recommendations[23] are bridging gaps in customer due diligence protocols of this industry.

21: Cipher Trace - Cryptocurrency Report 22: 6AMLD 23: AML Rules for Virtual Currency and Legal Sector – FATF 2019

Predictions for 2021

Overall decrease in fraud was surprising for team Shufti Pro as well. However, we noticed that some regions like Asia had a higher ratio of fraud in 2020. Unfortunately, identity theft was the rising issue in Asia more than any other region.

Synthetic Identity Fraud will Become Common

Synthetic identity fraud is accountable for up to 20% of credit losses and costs lenders millions every year, as stated by Auriemma Consulting Group.[24]

Synthetic identity fraud will increase in 2021 as identity fraud will become more sophisticated using advanced technologies. The mixture of fake and real biometric and document information makes it difficult to identify a synthetic identity. In-depth document screening and biometric authentication is required to capture synthetic fraud.

24: The Federal Reserve: Payments Fraud Insights, July 2019.

Replay Attacks will Proceed to Rise

Replay attacks are becoming more prevalent and proceeding to rise in the subsequent year. Imposters can bypass the device camera to embed stolen video, infect the machine with malware to intervene with the information being transferred or try to attack the API directly and transmit fraudulent signs there. Replay attacks are becoming more prevalent, companies will need more intelligent methods to cross-reference and authenticate identity signals. Continuous advancement of these signs will be a preference for companies and providers, which is why companies should utilize other means of verification, such as biometric authentication.

Deep Fakes will Hinder Biometric Proofing

Advanced identity fraud attacks like deep fakes are a point of concern for businesses. As many countries have now allowed video interview KYC there will be a rise in the usage of deepfakes to manipulate video based KYC screening. Authentic AI-based biometric authentication along with real-time human interaction is the key to capturing deep fakes. AI-based solutions, if trained well, could identify deepfakes through minor loopholes such as asymmetric skin patches, inconsistent lighting or glare on the iris.

Deep Fakes are continuously rising since 2017 and are expected to target businesses in the coming years.

Healthcare Fraud will Increase

COVID-19 pandemic increased uncertainty in healthcare and exposed the global medical infrastructure to an unpredicted risk. While several authorities such as FATF and FBI are warning people about COVID fraud, healthcare data breaches exposed millions of PHI records in 2020. These stolen records would most likely be used to conduct medical frauds, insurance scams and for illegal purchase of controlled medical substances. Given the rise in exposed medical records, enhanced patient verification will be inevitable in 2021.

One of the latest data breaches reported to HIPAA exposed 9.7 million[25] patient records in September 2020.

25: HIPPA Journal - September 2020 Healthcare Data Breach Report

Business Email Compromise (BEC) Fraud

BEC fraud is conducted to manipulate businesses into making unauthorized payments or releasing their secret information to fraudsters. Often criminals use illegally obtained or duplicate email credentials of businesses to demand payments from their customers or vendors. BEC fraud will be a point of concern for businesses in 2021, especially those which develop online B2B relations across the globe. The businesses must crosscheck with their vendor/partner before releasing payment or any information against requests received through email or call.

A report[26] found that payment and invoice fraud increased by 80% in the third quarter of 2020. While the median number of BEC fraud attacks per company each week increased by 15%.

26: Quarterly BEC Report

Re-victimisation

According to the latest data from the Federal Trade Commission (FTC), identity theft has risen to the number one scam during the COVID-19 pandemic[27].

Reports from Identity Theft Resource Center (ITRC)[28] have revealed that re-victimisation can be expected in 2021. Stolen identities in the previous years will be reused for more frauds this year. It seems the fraud is changing its targets. A huge number of public organization fraud was witnessed in 2020. As businesses reduced their activities during 2020, government organizations came forward to help people. Lack of IDV checks lead to increased fraud in the public sector. Looking at this trend we can predict that public service organizations will be the major targets of fraudsters. Stolen identities will be re-victimized to steal people off their benefits, insurance, healthcare and tax benefits.

27: ID Theft Surge During Pandemic 28: Identity Theft Resource Center (ITRC)

AI-Based Identity Verification Solutions

Secure Your Business in 2021

As monetary frauds are clamping up, the demand for identity verification technology is rising equally. The identity verification market is expected to reach a value of $12.8 billion by 2024 with a Compound Annual Growth Rate (CAGR) of 16.0% during the expected period.[29]

29: Identity Verification Market

KYC - Identity Verification

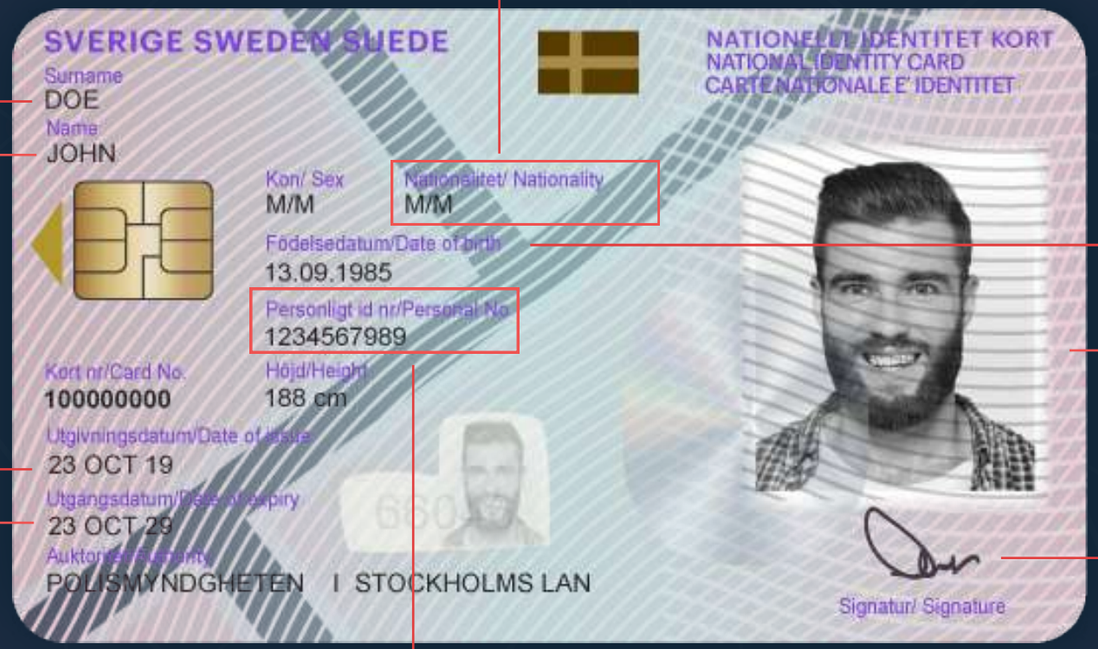
Shufti Pro is providing state of the art identity verification solutions for businesses, healthcare institutions, banks, real estate sector, and entertainment industry to fight multifaceted fraud. Our solutions use enhanced AI to detect multiple types of frauds (a few are discussed in the previous sections).

The KYC screening solutions provide multi layered security with document screening and biometric authentication in a single verification. The document is verified to evaluate the authenticity of the identity information provided by the customers, while biometric authentication performs liveness detection to ensure that the person is the original owner of the identity document. Artificial-intelligence-based face verification has the capacity to identify and fight facial spoofing attacks. With elements like liveness detection, 3D depth detection, and microexpression analysis, our deep-learning-based facial recognition software could accurately measure facial features.

The biometric authentication solution provides a quick and safe way to avoid account takeover fraud with selfie-based login. It not only enhances customer experience but protects businesses against financial and reputational losses from fraud. Explore identity verification solution.[30]

30: Identity Verification Solution

Document verification checks



Nationality

Face Photo

Last name

First name

DOB

Issue date

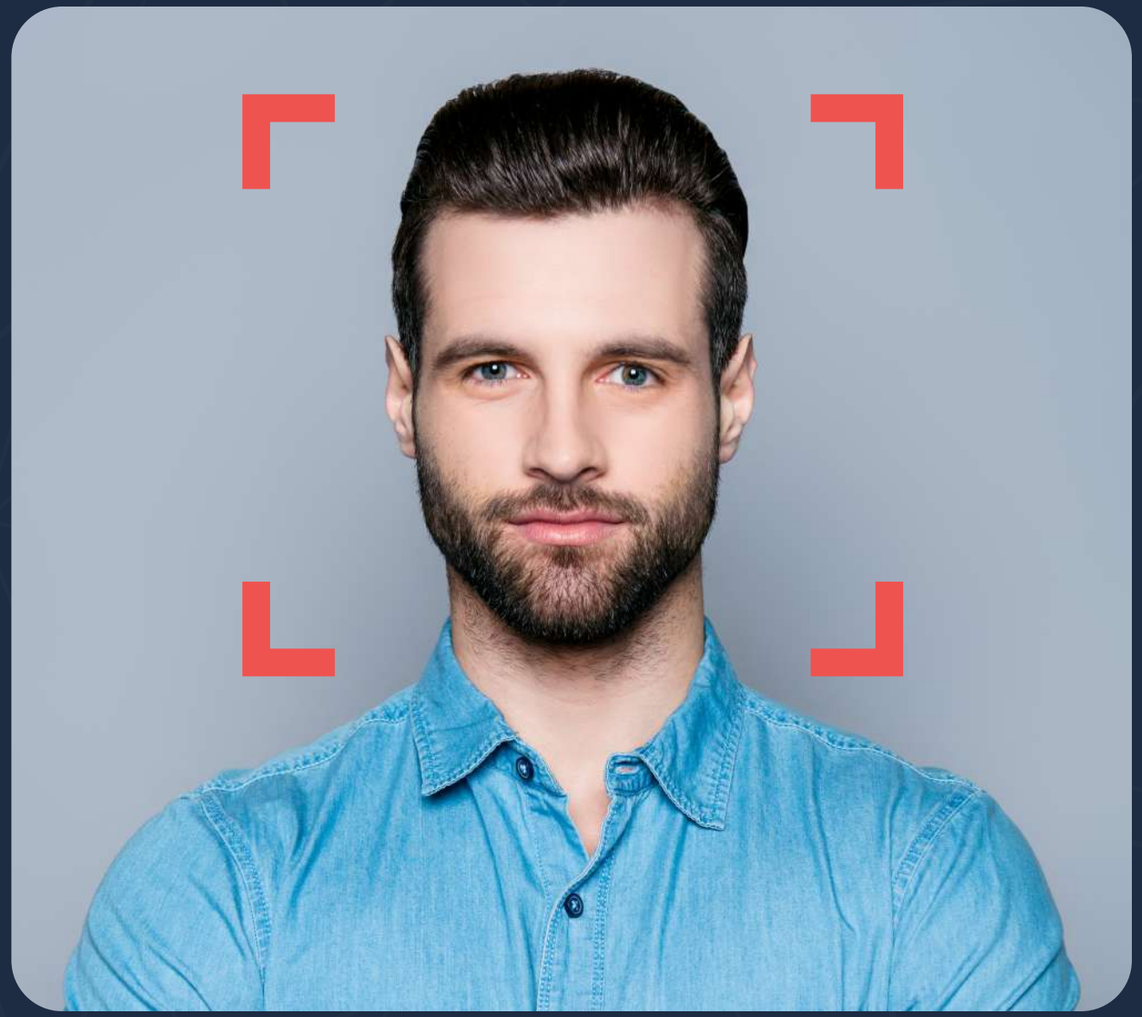
Expiry date

Signature

Document Number

- Check for accuracy of Format
- Check for authenticity of MRZ
- Detect crumpled / folded edges
- Check photoshop | tampering | forgery
- Verify hologram | rainbow print
- Detect blurriness | exposure
- MRZ or bar code
- Country of origin

ShuftiPro



Face verification checks

- Liveness detection
- Microexpressions analysis
- 3D depth perception
- Anti spoofing checks
- Fake image detection
- Human face attributes analysis

AML screening suite

The AML screening solution of Shufti Pro utilizes over 1700 official sanction and watchlists to screen the end-users. The AML screening solutions can help you screen existing clients in bulk or authenticate new clients in real-time. On the other hand, AML screening for businesses solution helps you develop secure B2B relationships around the globe by verifying business entities against watchlists and sanction lists.

Video Interview KYC

The video interview KYC solution is developed to fight advanced identity fraud. It helps the businesses to verify their clients through an online video call. The KYC expert interacts with the end-user in real-time and guides him to perform the verification. Video KYC is the advanced substitute for in-person identity verification, and allows businesses to expand globally without compromising their KYC/AML protocols. Shufti Pro provides multiple models of video KYC solution. You can equip your in-house KYC experts with our video KYC technology or utilise our agents. We provide regional and international KYC experts, you can get a shared or dedicated agent for the verification of your customers. Also, totally automated video KYC is another variant which performs AI-based video KYC without any human assistance. Explore solution[31]

31: Video Interview KYC

Key Takeaways

2020 was distressing for everyone and businesses have suffered a lot. Digitisation is the future of all organisations and robust customer due diligence is inevitable to fight frauds in 2021.

Preventing fraudsters demands enhanced IDV solutions like face verification, video interview KYC, and Know Your Business (KYB) to make sure everyone in the organisation is verified before onboarding.

Identity theft, account takeover fraud, money laundering, deep fakes, spoof attacks, 2D and 3D face masks were the most reported attacks in 2020. Finance, insurance, crypto, and the government sector face the most issues. The election season in the US was not secure either, and the mail-in-ballots were insecure without identity verification. One of the voting infrastructures in Georgia was under a ransomware attack as well. All these issues resulted in non-compliance with FATF guidelines.

On the other hand, banks and other financial institutions experienced a significant increase in identity theft. The online gaming sector reported more account takeover fraud issues than before. Lastly, the crypto sector experienced a rise in money laundering and reports estimated that 2020 broke records for crypto crimes.

We need better KYC and AML screening protocols across industries to ensure retainable growth in 2021 and beyond.

Incorporate Enhanced
Identity Verification

Try Demo

Get Information

Shufti Pro True Identity Builds Trust

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.