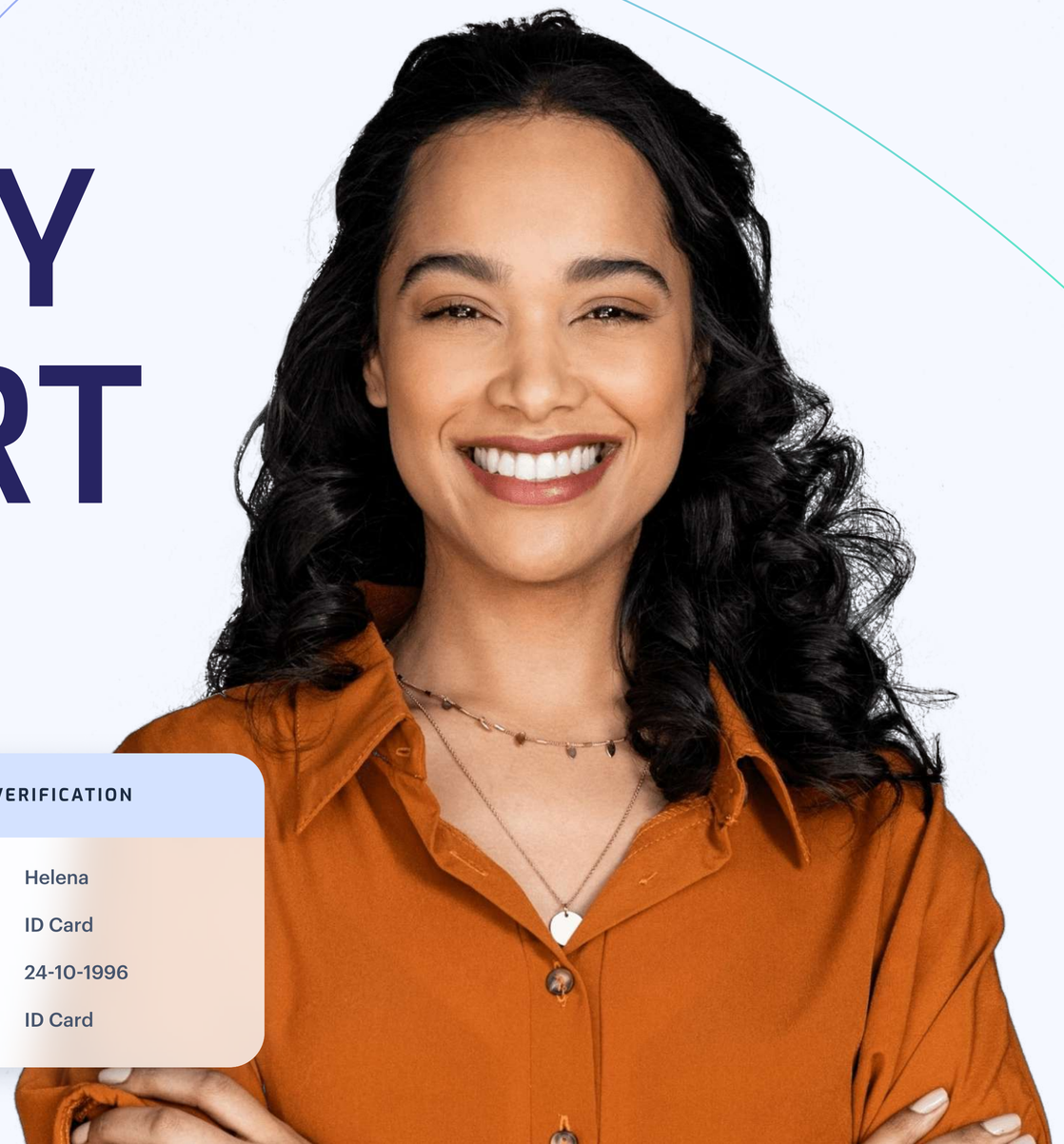
Shufti Pro

2022 IDENTITY FRAUD REPORT



Copyright © ShuftiPro Ltd. All Rights Reserved.

FOREWORD

Victor Fredung,
Co-Founder & CEO

During 2022, we have seen a heavy increase among fraudsters to manipulate documents, partly identity documents but primarily documents attesting to individuals proof of residence.

Fraudsters are getting smarter and are not using the standard pixel manipulation but we have also seen an increase in AI generated fraud manipulation. Nevertheless, as long as the anti-fraud industry stays up to date we will continue having an advantage over the fraudsters.

Shahid Hanif,
Co-Founder & CTO

The unprecedented levels of global ID fraud show no signs of slowing down. Our data analysis shows a year-over-year increase of slightly over 30% in Document fraud from last year. ID theft, authorised push payment scamps, fake documentation, and deepfakes are rampant among cybercriminals, making it extremely challenging for businesses to ensure KYC compliance.

INTRODUCTION

Hackers and cybercriminals are getting smarter by implementing sophisticated techniques to dodge the system. 2023 will be a challenging year as an increasing number of companies are on the radar of regulatory watchdogs.

The collapse of FTX, liquidity crunch in the crypto sector, and heightened risk of frauds in the gaming industry, ensures compliance will be a game-changer for 2023.

The unprecedented levels of global ID fraud* (Disclaimer at end) show no signs of slowing down; our data analysis shows a year-over-year increase of **30%** in document fraud ID theft, authorised push payment scams, fake documentation, and deepfakes are rampant among cybercriminals, making it extremely challenging for businesses to ensure KYC compliance.

The global fraud rate has increased year-over-year by **18%**, from **13%** in 2021 to **16%** in 2022.

Small and medium-sized organisations are an ideal target for hackers due to lack of stringent security measures put in place.

82% of all cyberattacks in 2021 were targeted at firms employing less than 1,000 people

Accenture's **Cost of Cybercrime Study** reports that **43%** of all cyber attacks are aimed at small businesses, yet only **14%** have sufficient defence mechanisms in place

Cybercriminals also target larger enterprises because one successful attack can result in damages tantamount to attacking multiple small businesses.

Understanding how fraud occurs critical in implementing the right data protection measures to safeguard identities and minimise the chances of data breaches.

An array of new data manipulation trends have emerged from the preceding year, but remote spoofing for fake liveness has especially captured our interest.

The first six months of 2022 saw **255 million social engineering attacks**, up by 61% from the same time period in 2021.

Failure to comply with regulations can often lead to severe legal consequences, including but not limited to penalties, business closure and loss of client value.

This report uncovers:

- Alarming Types of Fraud and Trends
- New Manipulation Techniques
- Our Recommendations on Remaining Safe

Fintechs are exposed to significant risk because of their digital process:

- Opening Mobile Wallet
- Verifying Customers Identity
- Allowing Bill Payment
- Disbursing Loans

This is a challenge for neobanks as they navigate the precarious ground to navigate of KYC and AML compliance.

Whilst banks and financial institutions already have CDD (Customer Due Diligence) in place, the swift move to digitalisation is now mounting pressure to adapt its digital means.

Post COVID-19 pandemic, the need for AI driven ID verification has escalated, from crypto exchanges to banks, sophisticated KYC methods have become critical to ensure regulatory compliance and minimise the risk of fraud.

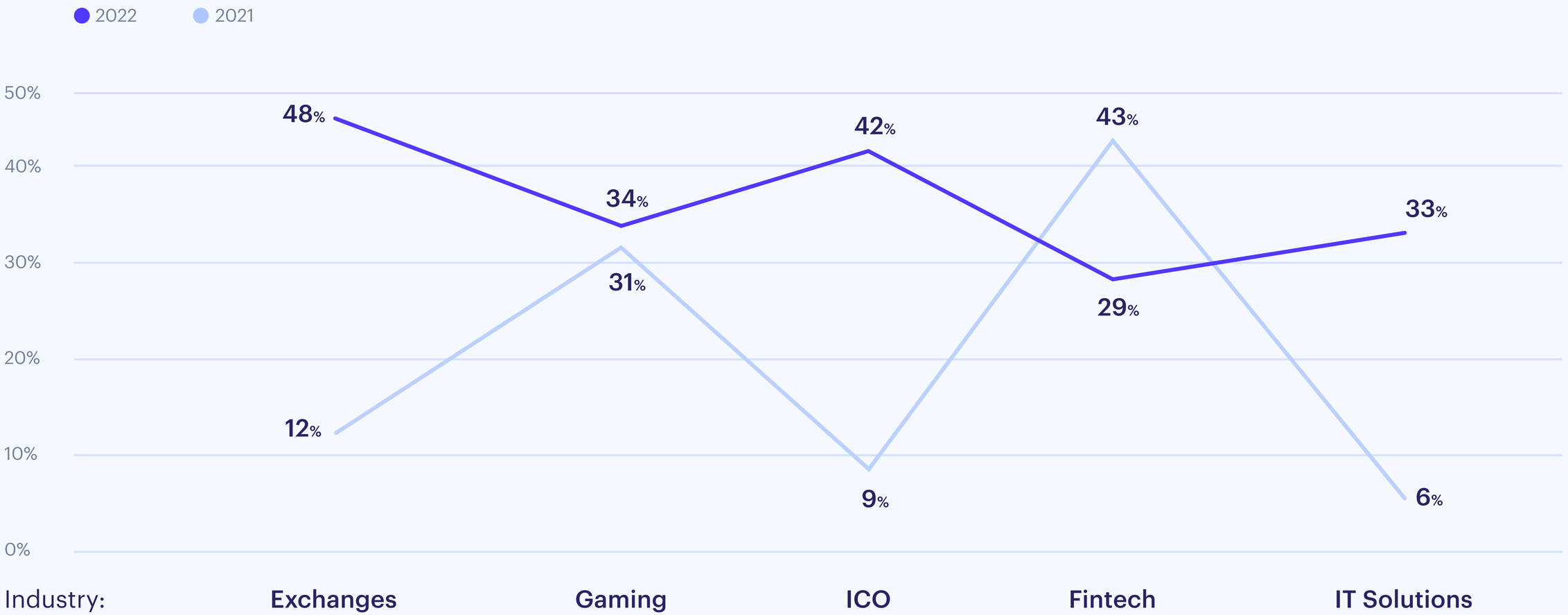
GLOBAL INDUSTRIAL OUTLOOK 2022

Over the course of 2022, Shufti Pro closely analysed fraud rates across numerous industries industries. The collapse of FTX and the rising scams in cryptocurrency has caused a steep incline in fraud rates fraud rates, from **12%** in 2021 to nearly **48%** in 2022. By far, this isn't just the biggest jump, but also the highest fraud rate across any industry that we worked with in 2022.

And the similar trend was seen in ICOs and IT solutions. With rug pulls and fraudulent activity in new coin offerings, the fraud rate skyrocketed from **9%** in 2021 to **42%** in 2022.

The IT industry felt another jolt because of fears of ransomware and having inadequate measures to ensure strong safety measures. As a result, there was a **450%** increase in fraudulent activity in the IT sector, from **6%** in 2021 to an astounding **33%** in 2022.

The crowdfunding industry had the highest fraud rate in biometric and document forgery, at **50%** and **42%** respectively; among all types, passports and ID cards dominated the highest amount of fraudulent attempts.



TAKEAWAYS FROM 2022

2022 was marred with an increasing amount of hacks

+12%

Losses have amounted to billions of dollars, from cryptocurrency to bank fraud, romance scam, ID thefts and government imposters; the total loss from global fraud has inflated from to **£3.89 trillion** in 2019 to **£4.37 trillion** in 2021

+233%

Cybersecurity Ventures estimates that by 2025, global annual losses resulting from cybercrime can **exceed $10 trillion**, up from **$3 trillion** in 2015

TOP FRAUD TRENDS BY CATEGORIES – MAJOR EVENTS AND HIGHLIGHTS

Shufti Pro's in-house analytics team have collected and dissected data acquired through 2022, spanning across all regions and industries. We've categorised our data by biometric and document fraud, alongside comparing trends in these categories across 2021 to 2022.

Document Fraud

Advanced forgery has taken many shapes, all in an attempt to bypass existing security measures. The most common documents used for verification are ID cards, bank cards, driving licences, passports, and work permits. Fraudsters are now leveraging the power of AI to tamper with bills and ID cards. In our analysis, using tampered and expired documents was the most common reason for rejection. 2022 was marked with the highest rise of ID document forgery at close to **24%** in 2022, compared to **18%** in 2021. This is an increase of more than **33%** within one year. Passports have taken the top spot in document fraud at nearly **40%**, compared to ID cards at slightly **26%**

Biometric Fraud

Our data analysis has demonstrated biometric fraud to have increased from **16%** in 2021 to **18%** in 2022. Deepfakes and other technologies are being increasingly used to outmanoeuvre KYC; this is because the AI technology used for biometric verification being sophisticated enough to detect spoofing attempts. Liveness detection is a sophisticated security measure which is difficult to bypass, causing hackers to redirect their efforts elsewhere. In this case, it was easier to shift focus to document fraud instead

DIGITAL BANKING FRAUD

UK Finance has declared bank fraud a **“threat to national security.”**

In the first half of 2022, consumers in Great Britain lost **£609.8 million**, a drop of **13%** from **$754 million** from the same period last year. UK Finance stated that rates of cybercrime would not decline, despite the decline in fraud losses.

The following table highlights the incidents of computer viruses and unauthorised access to Personally Identifiable Information from 2020 to 2022 in the UK:

YEAR	COMPUTER VIRUS	UNAUTHORISED ACCESS TO PI	TOTAL COMPUTER MISUSE
2020	360,000	504,000	863,000
2022	335,000	1,298,000	1,633,000

- The **Office for National Statistics (ONS)** states total fraud cases reported to the police in 2022 stood at **936,276**, compared to **797,897** in 2021, a rise of **17.3%**.
- However, the total computer offences and cybercrimes increased almost two fold, from **863,000** in **2020 to 1,633,000 in 2022**. This is primarily because of a rise in digital banking as widespread lockdowns restricted person-to-person interactions.

Consumers reported over **2.9 million** cases of fraud to the Federal Trade Commission (FTC) in 2021. Out of these, **1.43 million** were related to ID theft, which remained the top reported fraud

The situation of ID theft and bank fraud in the US is even grimmer, according to **AARP**, **42 million** Americans suffered a mammoth **$52 billion** in losses

Financial losses from ID theft and document fraud amounted to **$6.1 billion** for 2021. Figures for the first three quarters of 2022 have exceeded **$6 billion**, which is **44.73%** higher than the same period in 2021, despite a **26.76%** drop in reported cases

ID THEFTS – FTC

ID theft remains the top financial fraud, as per the data compiled from FTC:

THREAT	2021 (Q1-Q3)	2022 (Q1-Q3)
ID Theft	1,180,758	**864,699**
Total Fraud Cases	2,317,364	**1,692,139**
Total Loss ($ billion)	4,274	**6,188**

Consumers reported 864,999 ID theft incidents to FTC in the **first 3 quarters of 2022**, amounting to an eye-opening **$6.18 billion** in the amount lost.

It is also important to note that even though reported attacks have decreased, the intensity and damage for each one, has swollen remarkably.

ID THEFT TYPES	2021 (Q1-Q3)	2022 (Q1-Q3)
Government Documents	377,379	**46,439**
Other ID Theft	294,973	**256,298**
Credit Card Fraud	287,889	**338,684**
Loan or Lease Fraud	154,734	**121,708**
Employment Fraud	98,175	**85,124**
Bank Fraud	93,037	**120,481**
Phone or Utilities Fraud	68,669	**59,482**

2020 and 2021 saw a massive jump in US government's support payments to small businesses and families across the country during COVID19. It was at this time that fraud using government issued documents became the most dominant form of fraud.

However, in 2022, it dropped by **88%**, whereas credit card and bank frauds registered a sharp increase

AUTHORISED PUSH PAYMENT FRAUD

The Authorised Push Payment (APP) fraud is not new by any means, scammers have started using sophisticated methods to lure victims into believing calls are from a legitimate individual.

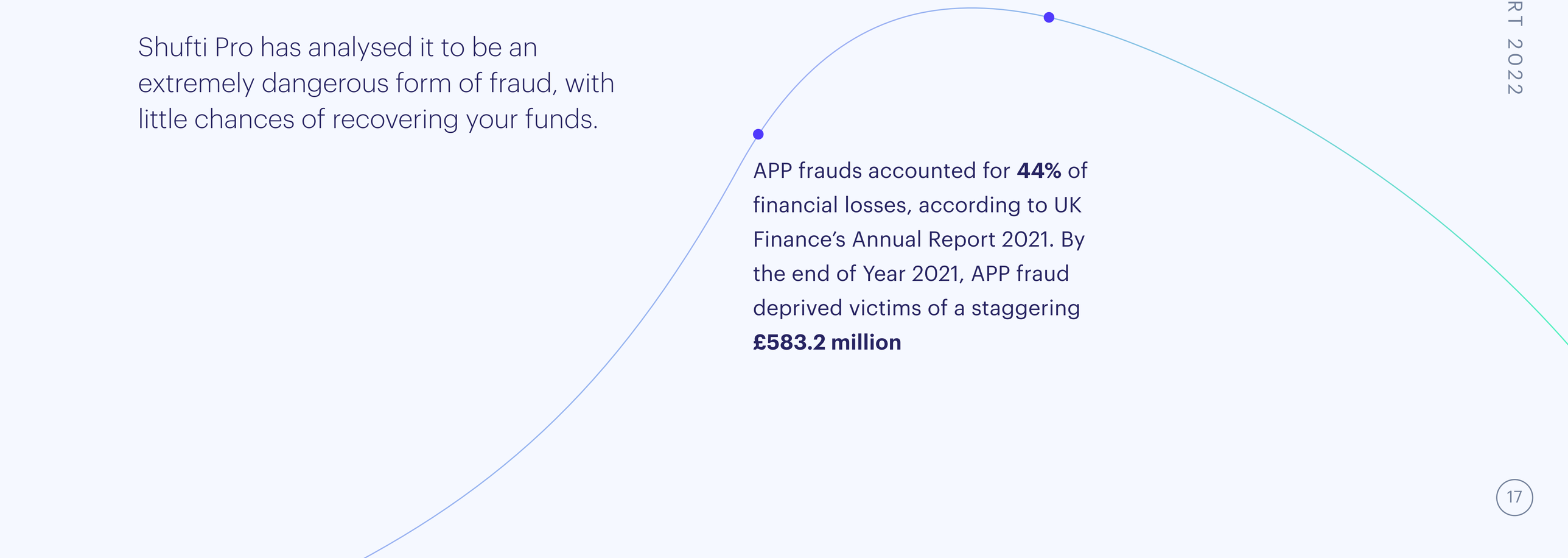
APP fraud happens when:

- The scammer convinces the victim to make a transaction
- The victim authorises the transaction to transfer funds to the scammer
- The scammer has complete control of the recipient's account
- Funds are then immediately transferred to multiple accounts, before criminals cash them out

This process makes it challenging for banks and law enforcement authorities to backtrace steps to the stolen funds.

No legislation exists to cover the losses resulting from APP frauds.

Shufti Pro has analysed it to be an extremely dangerous form of fraud, with little chances of recovering your funds.



APP frauds accounted for **44%** of financial losses, according to UK Finance's Annual Report 2021. By the end of Year 2021, APP fraud deprived victims of a staggering **£583.2 million**

Over **£600m was stolen** (UK Finance) in H1 2022. Out of this: **60% (£360m)** were APP scams

BANKING AND FINANCE INDUSTRY

- One reason for the surge in ID thefts and bank fraud in the US could be related to a record-breaking amount of branch closures, which started during the COVID pandemic.
- In 2021, there were more than **3,000 branch closures** in the US. The accelerated adoption rate of digital channels directly impacted bank fraud and ID theft.
- Banks in emerging economies are also moving away from paper-based to digital account opening.
- What took days now takes a few minutes. However, the process of scrutinising documents, verifying identification and KYC have proven difficult for the masses that are not digital literate enough to utilise technologically literate channels.

Price Waterhouse Coopers reported that **52% of organisations** with global annual revenues exceeding **US$10 bn** witnessed fraud within the last 2 years

$50 million per incident is the cost of business disruption

Cybercrime is also the leading type of attack **(42%)** on organisations with global annual revenue in between **$1 billion** to **$10 billion**

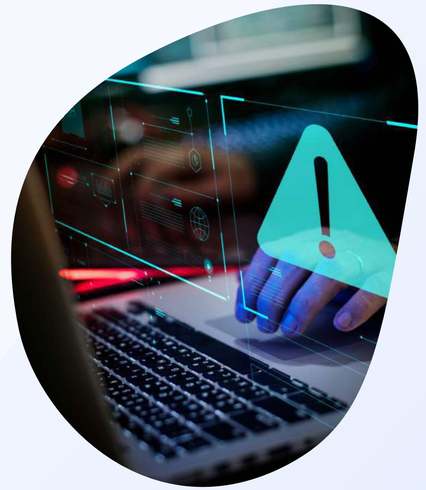
CRYPTOCURRENCY

2022 was the Wild West for the crypto market. Accompanied by a deregulatory environment and a blood bath for investors, the crypto market wiped out billions of dollars worth of hard-earned investor funds.

- The collapse of **FTX**, a **94% drop** in sales volume of Opensea, and the Terra Luna crash, all jolted the already volatile industry struggling to retain its credibility and legitimacy.
- Over **$3 billion** has been vanished by hackers in more than 125 hacks in the Year 2022.

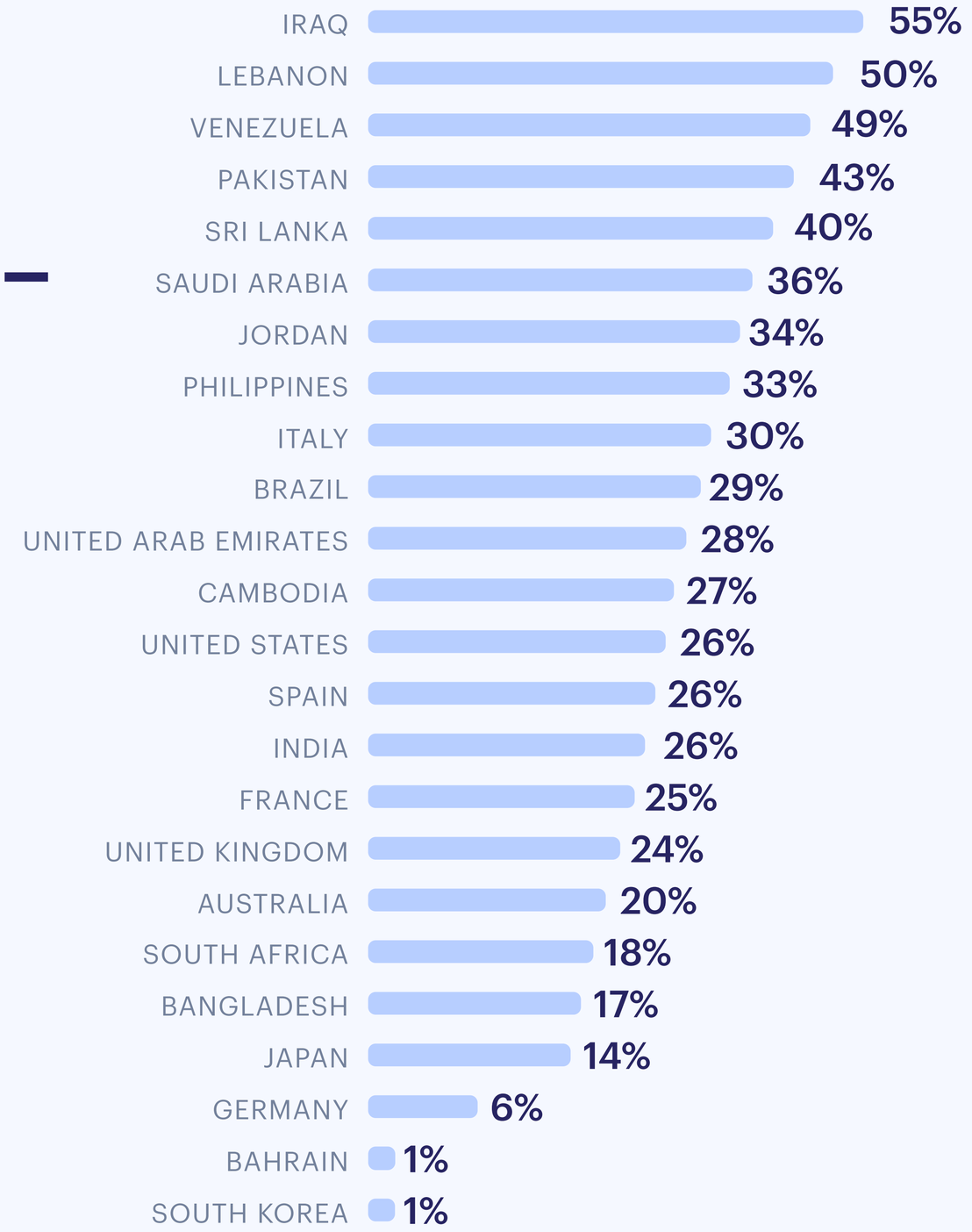
TOP FRAUD TRENDS IN 2022

Fraud continued in an upward trend in 2022, showing no signs of slowing down. The utilisation rate represents the proportion of the document type used for verification relative to the total number of attempts.



GLOBAL FRAUD RATES – COUNTRY WISE

Our analysis showed that Iraq had the highest global fraud rate of all types (**55.14%**), whereas Bahrain and South Korea had the lowest, at less than **1%**.



TOP MOST FORGED ID DOCUMENTS

2022 saw a surge in document forgery, with passports taking the top spot, followed by ID cards, at nearly **40%** and **26%** respectively. The document fraud rate was at **24%**, an increase of over **30%** from 2021's figure of **18%**.

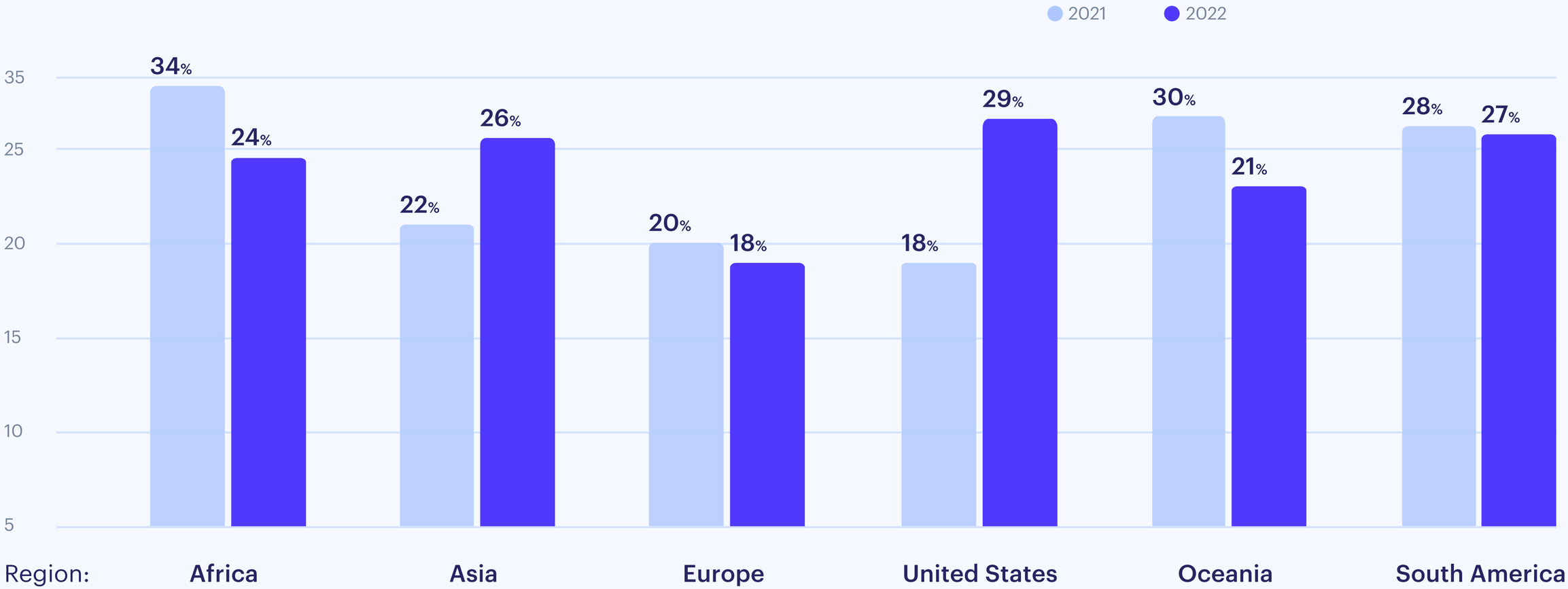
Pakistan, India, and China took the top 3 spots with the highest fraud rate using passports, at **41%**, **40%**, and **39%**, respectively. The same is true with the ID cards. Pakistan and Saudi Arabia also registered the highest fraud rate at **48%**, documents from these countries had the highest tampering rate.

Document Type:

- **39%** Passport
- **26%** ID Card
- **15%** Credit or Debit Card
- **23%** PR Permit
- **22%** Driving Licence

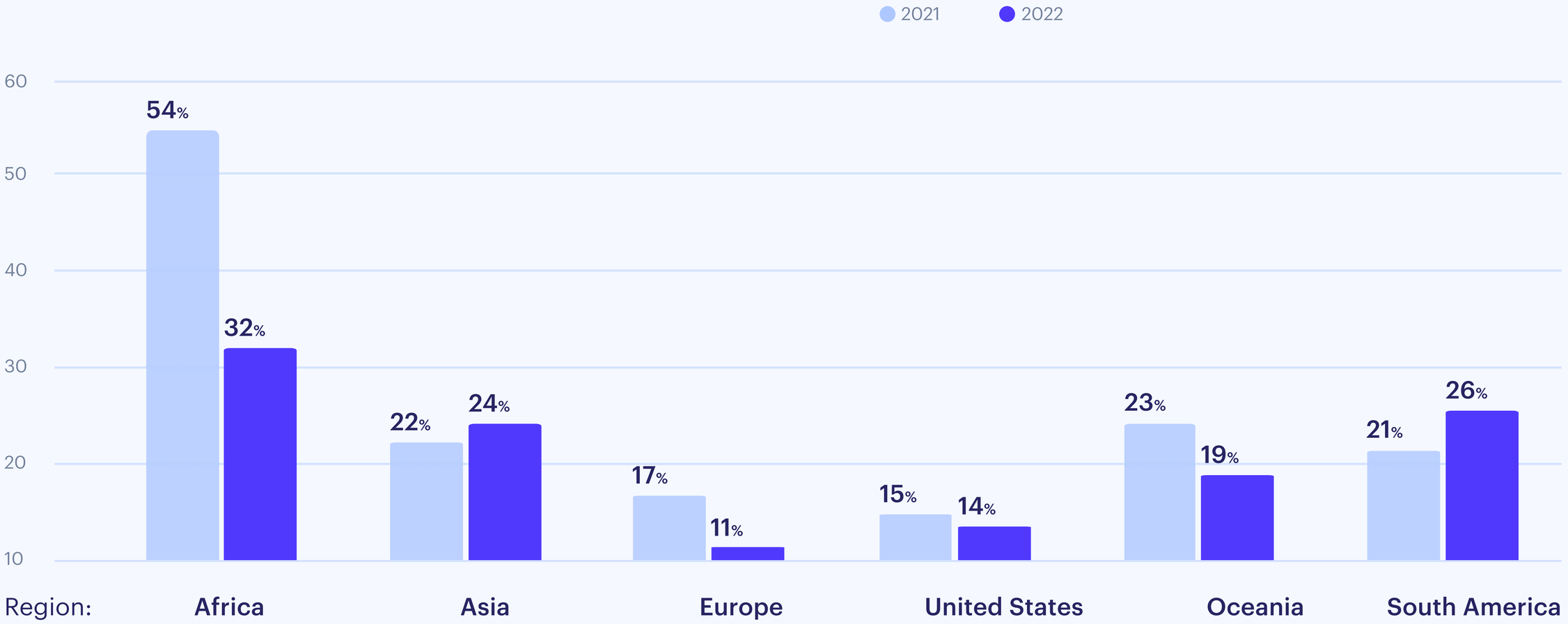
GLOBAL DOCUMENT FRAUD – REGION WISE

The US has seen a significant jump in fraud rates from **18%** to nearly **30%**. However, fraud rates decreased in Africa from **34%** to less than **25%**.



GLOBAL BIOMETRIC FRAUD – REGION WISE

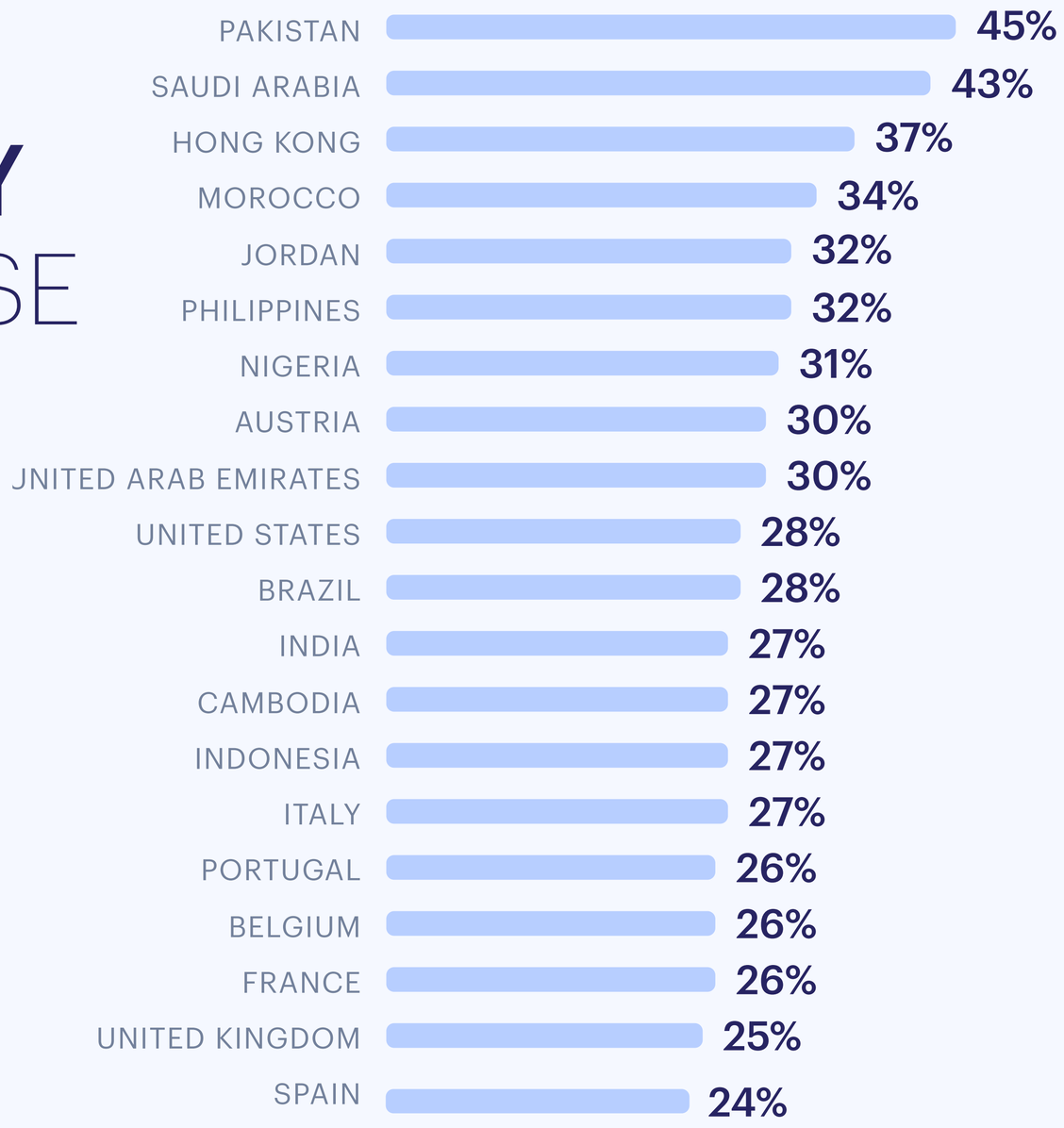
In our research, Africa had the highest fraud rate in 2021, in comparison to 2022 whereby it dropped significantly. However, Europe and South America registered an increase in biometric frauds.



DOCUMENT FORGERY RATES – COUNTRY WISE

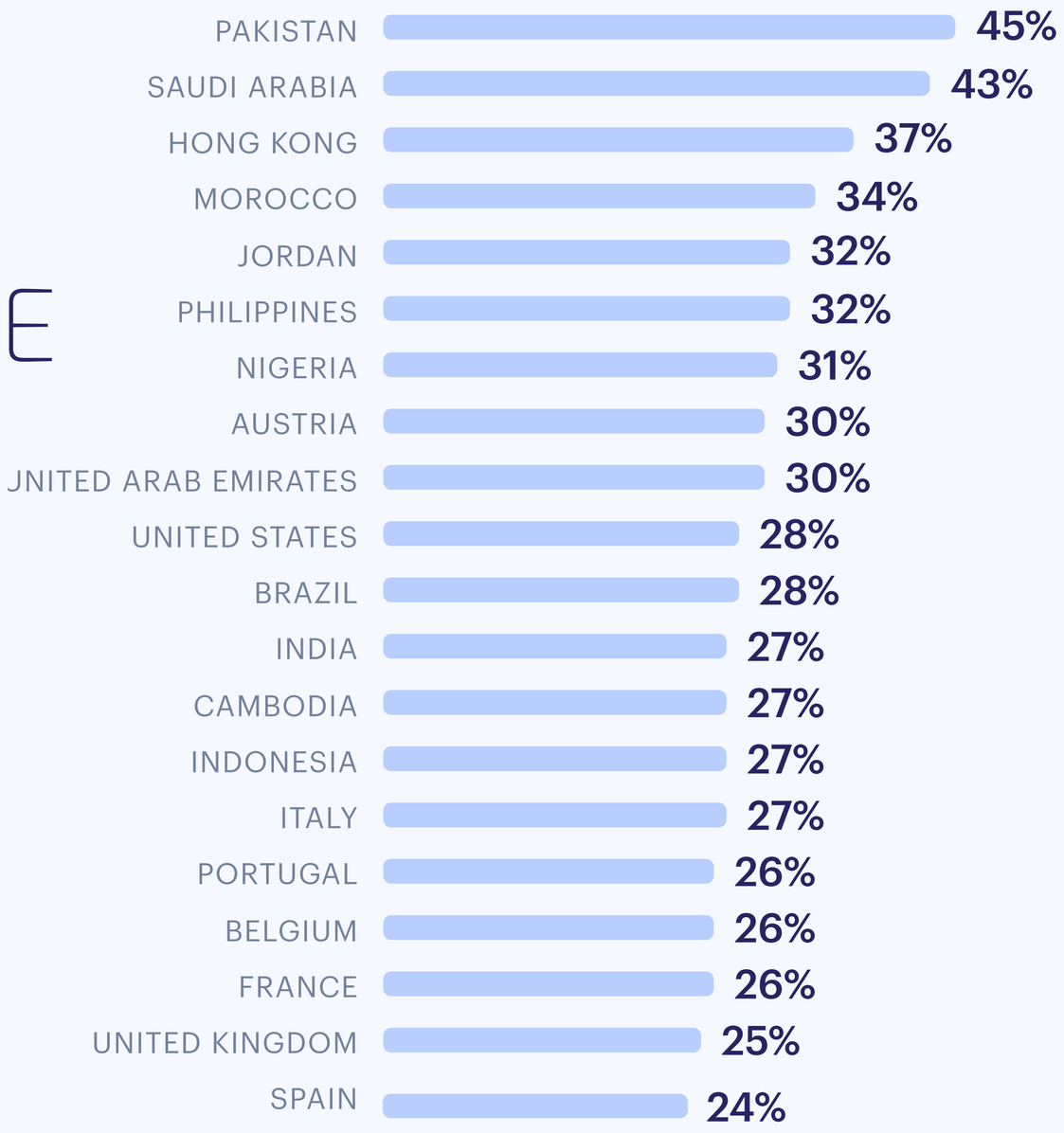
Document forgery is categorised as an attempt to tamper with ID documents to bypass the verification system, such documents can be passports, ID cards, bank cards, work permits, and driving licences.

Pakistan, Saudi Arabia, and Hong Kong had the highest document forgery rate at **45%**, **43%**, and **42%**.



BIOMETRIC FRAUD RATES – COUNTRY WISE

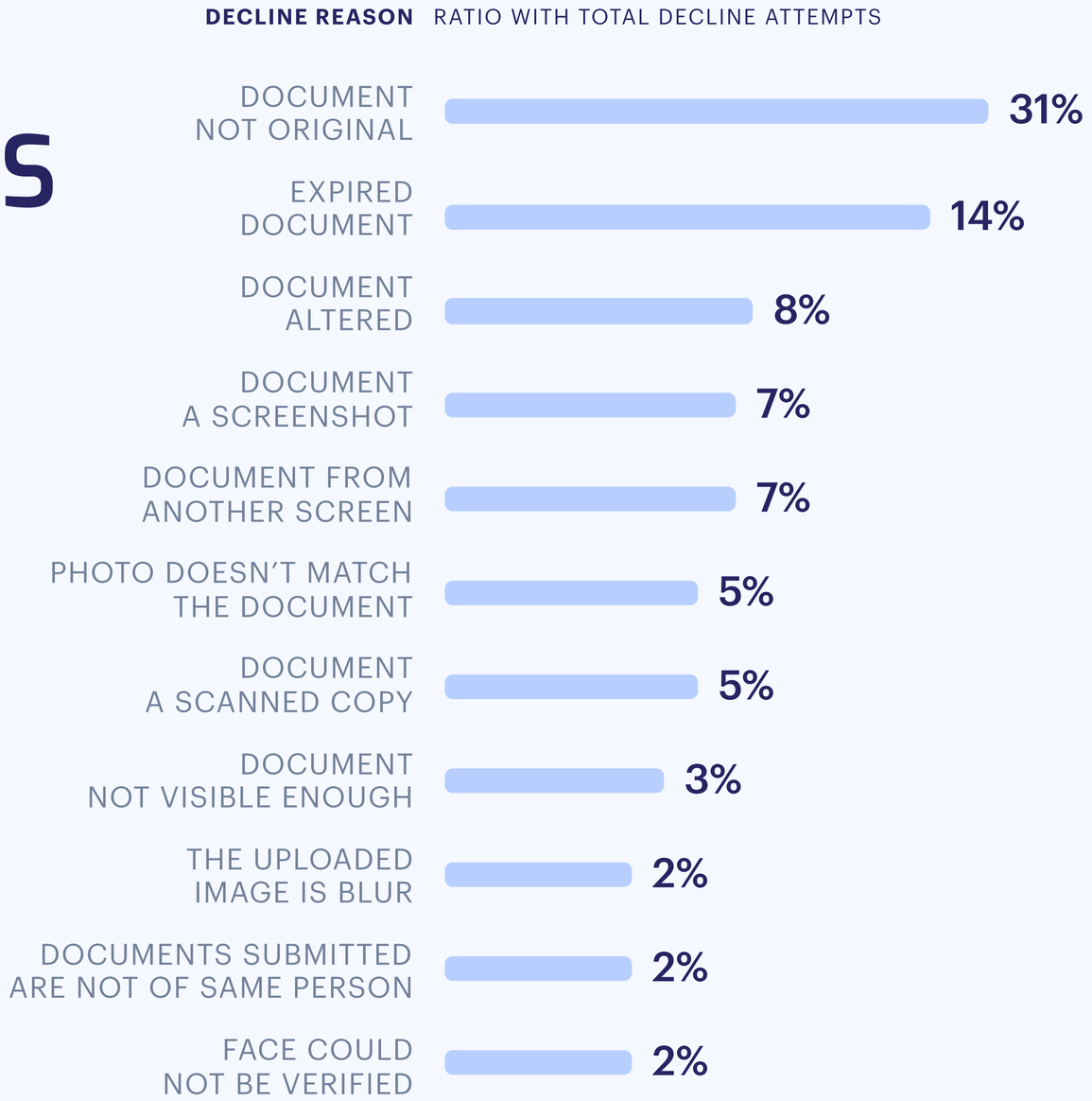
Iraq had the highest rate of biometric fraud, followed closely by Syria and Pakistan, at **60%**, **50%** and **47%**.



TOP DECLINE REASONS

Document tampering was the single most common reason for rejected verification attempts, followed by expired documentation. In total, just these two reasons contributed to nearly 50% of all declines.

This shows that verifying document originality will be a big challenge for businesses in 2023.



WHAT TO EXPECT IN 2023?

Fraud has quickly grown into a multi-billion dollar industry, banks, crypto exchanges, governments, educational institutes, and even hospitals have become the equivalent of digital darlings for hackers. These institutes are lucrative due to the nature of the highly sensitive and valuable data.

Deepfakes, remote spoofing for liveness, and ransomware remain the biggest threats for companies, individuals, and governments. As we navigate the murky waters of 2023 filled with increasing compliance challenges, we need to deploy powerful and intelligent AI-based KYC and KYB solutions to decrease the chances of being compromised.

The 30-39 age group reported the most frauds in 2022, slightly higher than 2021

NEW DATA MANIPULATION TECHNIQUES IN 2023

Shufti Pro has discovered new data manipulation techniques given the ever-growing nature of ID thefts and cybercrimes in 2022.

We expect the following to continue gaining momentum in 2023. Businesses and governments alike need to keep an eye for these type of fraud:

Remote hacking for fake liveness

Hackers can now stage successful biometric attacks in an attempt to outsmart the ID verification system, through **deep fakes and morphing**. The challenge-based liveness detection is difficult for hackers to overcome, but new methods are constantly being devised to bypass this safety mechanism by remote spoofing.

Liveness detection makes it possible for Shufti Pro and our team to determine whether or not the biometric trait presented is coming from a living person or a deep fake.

Remote hacking for liveness detection happens when an SQL injection takes place remotely after taking control of the smartphone application. Hackers can take the victim's picture using social media, and place it on top of the subject's video. More and more sophisticated AI models need to be made to detect and thwart attempts of remote hacking.

Here are some of the ways we use liveness detection to determine the legitimacy of the individual:

PUPIL DILATION

DETECTING TEXTURE

USING 3D CAMERA FOR FACE MAPPING

MOTION DETECTION OF THE MOUTH, EYES, AND THE HEAD

Stolen IDs

Stolen IDs or account takeover happens when the victim falls prey to the scammers and provides sensitive financial information, such as credit/ debit card numbers, and bank account credentials. The scammers, who often pretend to be calling from the “central bank”, proceed with account takeovers, bypassing all safety mechanisms, and initiating transfers.

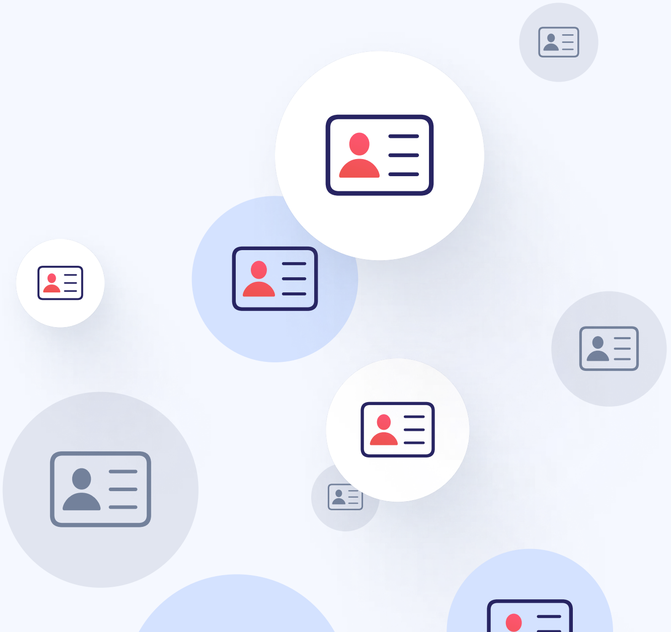
- Nearly **47% of Americans** have faced some form of identity theft, a rate that is 3 times higher than the rest of the world.
- Out of a total of **5.97 million** fraud reports to the FTC in 2021, **1.43 million** were related to ID thefts only.
- Figures for 2022 aren’t impressive either. The first 3 Quarters of 2022 showed **3.71 million** fraud reports, with **864,000** of those related to ID theft.

Duplicate IDs

- When an individual enrols several times in a system, there will be more than one instance of ID, this is called identity duplication.
- While it is common to have multiple entries of the same individuals under different characteristics, it is not a recommended practice; having duplicate entries gives cybercriminals a window to commit identity fraud.
- This is a rising trend our data revealed in 2022, and one we expect to continue in 2023.
- Businesses need to implement identity deduplication, a method used to remove an individual's duplicate entries from the system. It is critical for your business to deduplicate entries because multiple accounts can be used to commit frauds.
- Social media, specifically Meta's Facebook, is increasingly used to impersonate an individual for illicit gains.

In the **first two quarters of 2022**, the social media behemoth took down **1.6 billion** and **1.4 billion** duplicate/fake profiles respectively

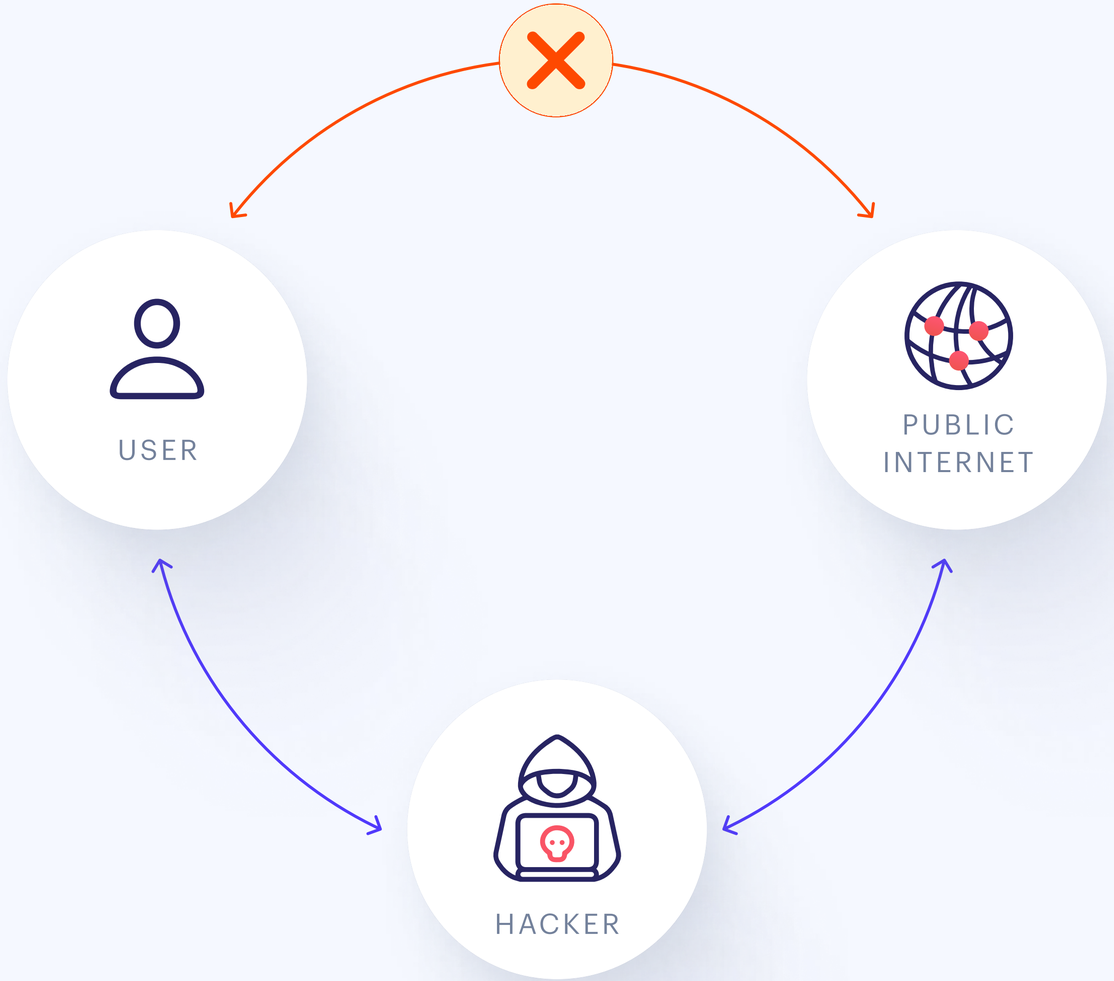
These profiles were created to impersonate a celebrity, political figure, and legitimate business or a charity.



Man in the middle attack

A man in the middle attack happens when the hacker, a third-party, listens to the communication between the communicating parties and gets access to all information. Neither parties know the presence of the third-party while sharing sensitive data.

Phishing attacks are specifically done with the intent of luring victims in sharing sensitive financial data over a communication channel such as phone calls and/or emails.



Ransomware

Ransomware has destroyed enterprises and is the biggest menace of the cybercrime world. According to the US Govt., **60%** of all small and medium companies go out of business within the first six months of a cyberattack.

623.3 million ransomware attacks happened worldwide in 2021, with a slightly more than double than in 2020.

At the time of writing this report, ransomware attacks have dropped by **23%**, which could be a result of tightened government regulations.

BIGGEST DATA BREACHES

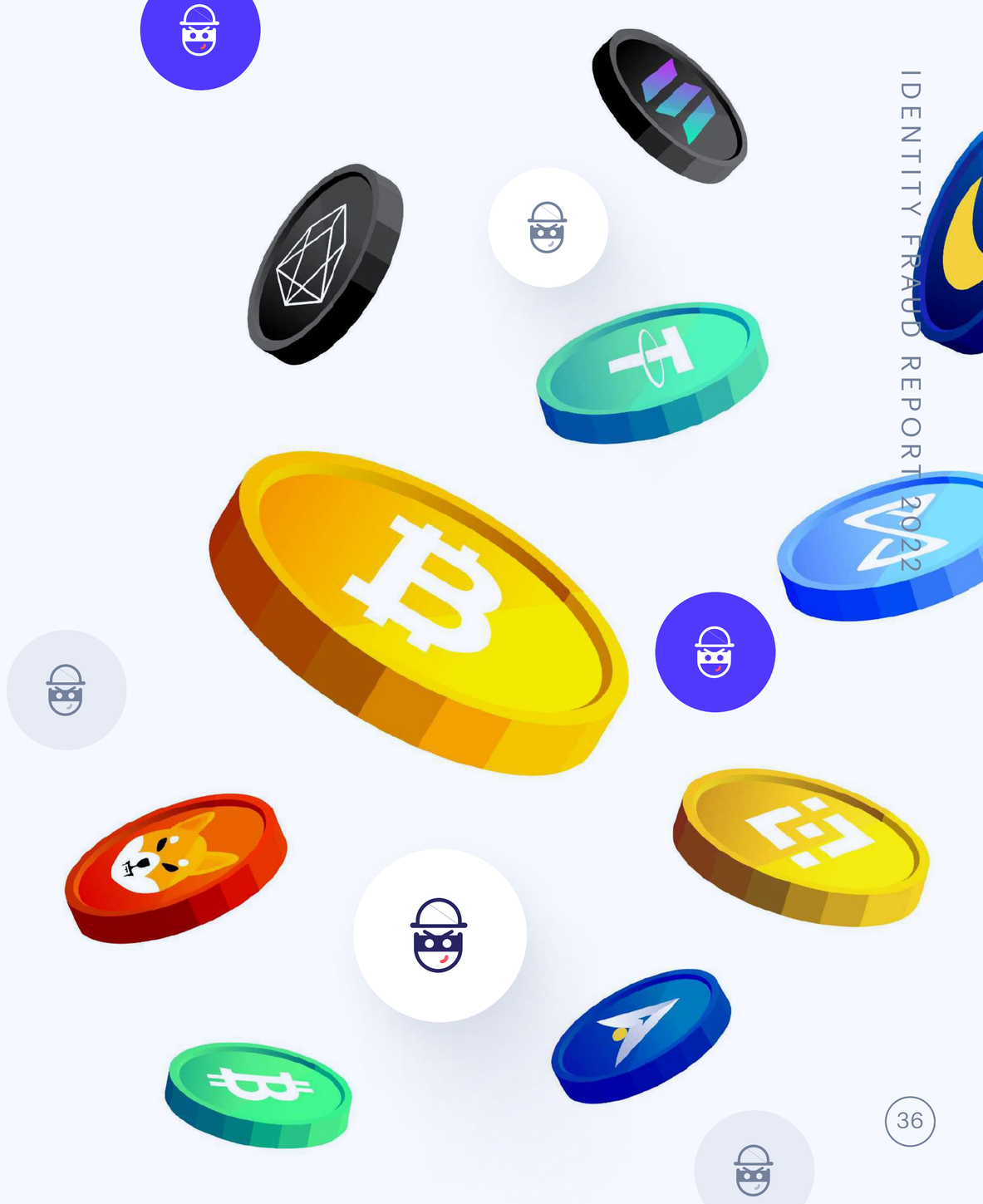
2022 saw some of the biggest data breaches spanning across various industries. Governments, corporations, and banks were all targets of hackers, leveraging the sweet spot of digitisation.

Cryptocurrency

What happens when you mix a lucrative fake job offer with the innocence of an employee looking out to advance in his/her career? A **$620 million heist.**

A carefully orchestrated, and well-played strategy of North Korean hackers successfully managed to wipe out over half a billion dollars in what is considered to be the biggest crypto hack till date.

Hackers exploited the Ronin network, a sidechain built on Ethereum, to steal cryptocurrency. Axie Infinity had nine validators, and the hackers needed to gain control for a complete account takeover. Sky Mavis, the game developer for Axie Infinity, has since started refunding the amount to its customers.



Government

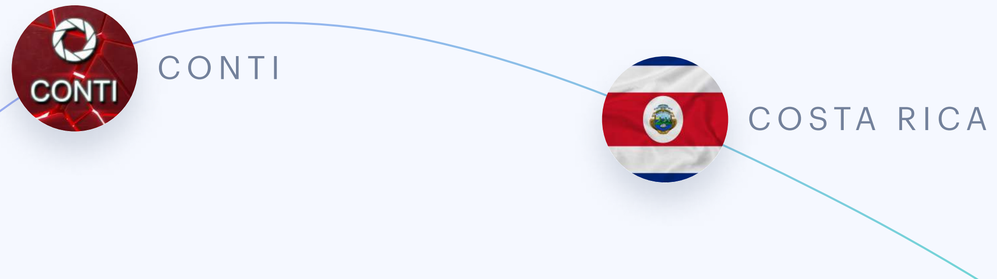
It is no surprise to see governments on the list of top data breaches for the year 2022. Hackers repeatedly make governments their targets due to the sensitive information of citizens in the database, such as Names, Social Security Numbers, Address, and more.

Conti Group, a nefarious criminal organisation, on **17th April 2022**, staged successful attacks, targeting dozens of Costa Rican government institutes. Costa Rica's government rejected the group's demand of **paying $10 million** in ransom to get back the data of citizens' tax returns.

Another attack took place on **31st May**, targeting the Costa Rican Social Security Fund. This time, the Hive Ransomware Group, the criminal organisation behind the attack, was looking to extort the government for **$5 million**.

Most of the government's official departments were impacted severely. To mitigate the attack and minimise the damages, the government had the entire network and official websites shut down.

The impact was staggering, with losses exceeding over **$30 million** in a matter of weeks.



BEST FRAUD DETECTION PRACTICES

Users are the best line of defence against fraud. According to our analysis, here are some tips you can implement right away to reduce your chances of getting compromised.

Use 2FA with Liveness Check

2nd factor authentication adds an extra layer of protection whenever a user attempts to sign in from a new device, location, and IP address. This ensures that the user is signing in to their own account and not anyone else's

Monitoring Accounts

Keep a close look at your company's official bank accounts, and always report anything suspicious to the bank without any delays. Only provide financial access to authorised users and implement multi-factor authentication

Implement Account Deduplication

Organised fraud attacks have exploded in recent years due to the re-use of same ID information. For example, they bombard the system with multiple verification requests having the same/ similar face or document numbers.

This is a type of brute force attack that tries to bypass the system. Luckily, Shufti Pro has advanced AI-based fraud detection systems in place to detect and mitigate this type of attack

ABOUT Shufti Pro

Ready to tackle the KYC/AML challenges of 2023? Learn how your enterprise can mitigate these attacks with a **99.3%** accuracy level, by partnering with Shufti Pro.

Available in over 230+ countries and territories, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure

Utilising the power of 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, KYI**, **eID**, **Address verification**, 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

EXPLORE OUR IDENTITY VERIFICATION SOLUTION

TO KEEP FRAUDSTERS AT BAY






Get Trial

Contact Us

* Disclaimer:

These findings are based on our clients' data that Shufti Pro collected throughout the year ending 2022. This time however, Shufti Pro managed to get a bigger picture with an in-depth analysis of all countries and regions as compared to the limited data for 2021.

No warranty or claim herein provided that information contained in this document is accurate, up-to-date, and/or complete. All information provided in this document is limited for general informational purposes only. In no circumstance(s), does such information constitute legal or any other advice. Any individual or company who intends to use, rely, pass-on, or re-publish the information contained herein in any way is solely responsible for the same and any likely outcomes. Any individual or company may verify the information and/or obtain expert advice independently if required.

Shufti Pro

Ready to utilise our Global Trust Platform for your KYC requirements?

Get in touch with our KYC & AML experts to learn how our solutions can be seamlessly integrated into your existing processes.

shuftipro.com

sales@shuftipro.com

United Kingdom

Office 409 Coppergate House, 10 Whites Row, London E1 7NF

United States

67 S Bedford St #400w Burlington, MA 01803

Sweden

Bröderna Pihls Gränd 2, 252 36 Helsingborg Skåne county

Dubai

Unit 507, Level 5, Gate District Precinct Building 03, DIFC, Dubai

Cyprus

Arch. Makarios III Avenue 229 in Limassol

Hong Kong

8 Queen's Road East, Wan Chai, Hong Kong