ENTRUST CYBERSECURITY INSTITUTE PRESENTS

2025 Identity Fraud Report

ENTRUST

onfido
an Entrust Company

Contents

Foreword

Understanding identity fraud trends is more critical than ever. Businesses are facing new and emerging techniques that are opening novel threat vectors, and these threats are rising at an unprecedented pace with the potential for existential impact.

The 2025 Identity Fraud Report from the Entrust Cybersecurity Institute provides a comprehensive look at the use of AI-powered techniques fueling cyberattacks and offers strategic guidance to help businesses make sense of these trends to stay protected in a world in motion.

Siddharth (Bobby) Mehta

Entrust Board Chair and former CEO of TransUnion and HSBC America

Emerging threats catalyzed by the rise and availability of generative AI tools – like the spread of deepfakes – are increasing pressure on businesses to catch sophisticated fraud vectors compared to previous years. The findings from this year's annual Identity Fraud Report reveal a deepfake attempt happened every five minutes in 2024, while digital document forgeries increased 244% year-over-year.

These trends should be deeply alarming for businesses, governments, and individuals. The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) issued an alert on November 13, 2024, aimed at helping financial institutions spot and fight deepfakes. Citing use of deepfakes created by generative AI (GenAI), they noted that:

> "FinCEN has observed an increase in suspicious activity reporting by financial institutions describing the suspected use of deepfake media, particularly the use of fraudulent identity documents to circumvent identity verification and authentication methods."

Efforts by governments and reports like this one put a much-needed spotlight on these rising fraud threats. Recent data predicts that the global cost of cybercrime – including fraud, scams, identity theft, breaches, ransomware, and more – is projected to hit an annual $10.5 trillion by 2025, according to Cybersecurity Ventures.

This drastic shift in the global fraud landscape underscores that strong digital identity verification is vital for businesses to stay ahead of bad actors and protect customers during the onboarding process from account takeover or fraudulent transactions. This year's report highlights why businesses must enhance fraud prevention and build defenses against deepfakes and other AI-driven attack vectors into the entire customer lifecycle.

This report by Entrust is remarkable in that it brings actionable, real-world intelligence on the changing nature of fraud, with insights based on proprietary data from Onfido, an Entrust company. In addition, the report offers organizations the tools they need to make informed decisions about how best to protect themselves – and their customers – from the ever-increasing and evolving threats of fraud in our digital and connected ecosystems.

Executive Summary

Fraud is a problem that has wide-reaching impacts for businesses, governments, and individuals alike. It's a fear when it's not happening, and it's a huge problem when it is.

Fraud is also not static. As we moved online, the threats changed. As technology evolves, the threats continue to change. Traditional forms of fraud have given way to more complex and innovative techniques, including synthetic identity fraud, deepfake technology, and fraud-as-a-service platforms. As a result, fraud-prevention methods have had to change to keep pace.

With a lens on onboarding and identity verification, this report explores some of the identity fraud patterns and trends that are impacting organizations today. It also examines emerging fraudulent techniques, including the impact of digitalization and the rising threat of fraud driven by artificial intelligence (AI).

Combining in-depth data analysis and input from internal and external fraud experts, this report offers business leaders, compliance officers, and security professionals strategies to enhance their fraud prevention – helping them stay ahead of fraudsters who continue to adapt their tactics into 2025 and beyond.

Methodology

Digital identity verification is a crucial step in any onboarding process when it comes to stopping fraud and financial crime. This first moment of interaction is an organization's opportunity to build trust in that identity from day one. In other words, identify genuine humans from the fraudsters.

Through Onfido's solution, Entrust processes millions of identity verifications each year, helping save an estimated $5.5 billion in fraud losses for our global client base. Access to this proprietary data also gives us unique insights into the latest trends in identity fraud.

The data analyzed in this report is from the one-year period from September 1, 2023, to August 31, 2024, and is derived from tens of millions of verifications across 30+ different industries in 195 countries.

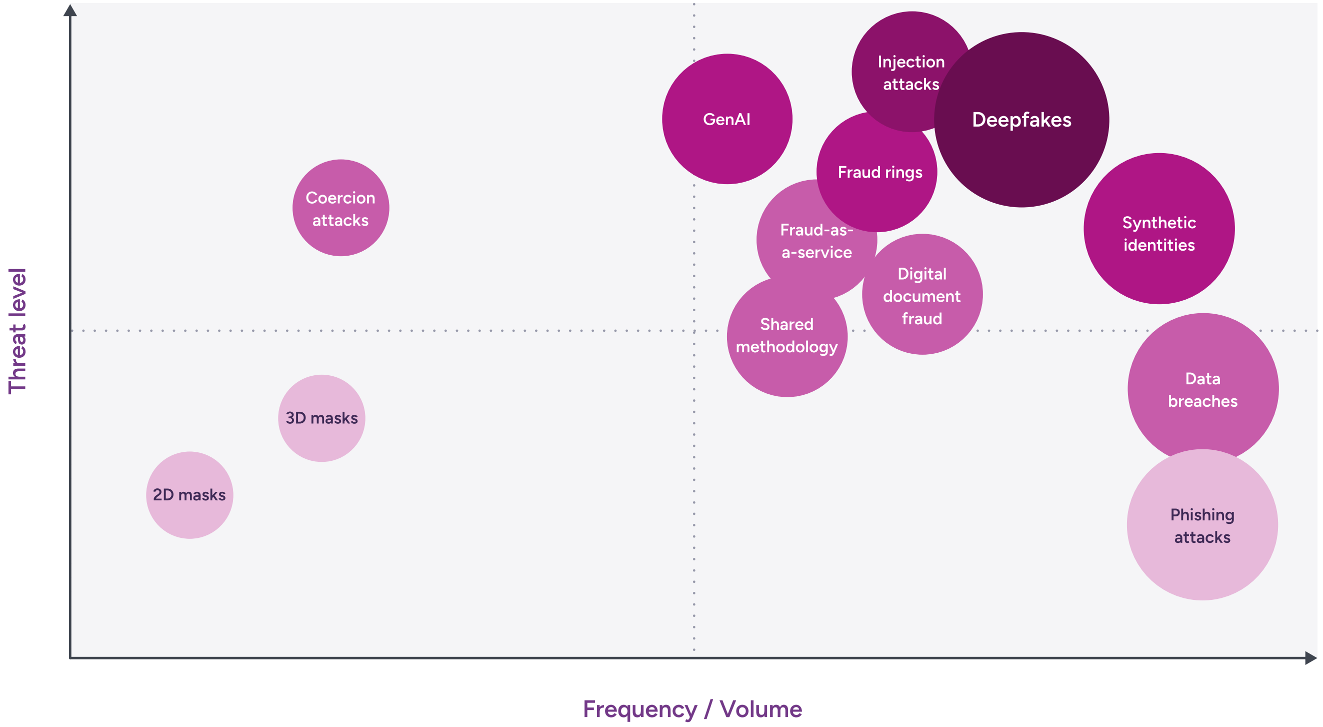
In some cases, we compare the data to previous years to get a better and more accurate understanding of the overall trends. The data and trends are reflective of the verification space and might not always mirror wider market trends. We retain the right to publish this data.

2024 Fraud Landscape

The state of fraud in 2024: from rising to established threats

The fraud landscape is constantly changing as fraudsters adapt and innovate their techniques to find new ways through defenses. New attack vectors emerge that pose heightened threat levels alongside patterns that have been well-established for years.

This graph shows some of the fraud vectors posing the highest risks to businesses in 2024. It's important to note that any type of fraud poses a risk; however, some of the emerging vectors are threats that businesses may want to pay particular attention to right now.



What's particularly concerning is that more and more fraudsters are using a combination of attack vectors, such as:

- ✓ Leveraging personally identifiable information (PII) obtained through data breaches and phishing to create synthetic identities
- ✓ Fraud rings sharing methodologies and offering fraud-as-a-service to arm more amateur fraudsters
- ✓ Fraudsters submitting deepfakes via injection attacks

Potentially, all of the attack vectors in the chart could be combined.

Fraud is becoming more complex and multi-layered, and therefore requires a multi-pronged approach to prevent it.

Key Findings

1. **Digital manipulation replaces physical document fraud**

This is the first year where digital techniques have replaced physical fraud across fake document creation. Historically, fraudsters would typically create new physical counterfeit documents from scratch. But for the first time ever, fraudsters are creating more digital forgeries than physical counterfeits, with digital forgeries increasing 244% year over year. This is a trend that's been brought about by the availability of AI-assisted tools, shared methodologies, and the rise of fraud-as-a-service.

2. **AI-assisted fraud is on the rise**

AI is not new, but there's been an increasing focus on how fraudsters are using AI to their advantage over the last few years. Whether it's generative AI (GenAI) tools creating convincing phishing emails, or producing realistic deepfakes with face-swap apps, or sites claiming to create realistic fake documents, there's a general consensus that AI is increasing the scale and sophistication of fraudulent attack vectors. And this shows up in the data: Digital document forgeries increased 244% in the last year, and deepfakes now account for 40% of all biometric fraud.

3. **Fraud is getting more sophisticated … and more accessible**

The use of AI, deepfakes, and techniques like injection attacks are all contributing to a rise in sophisticated fraud. At the same time, from fraud to ransomware to phishing and beyond, cybercriminals are embracing as-a-service models to up their own game and that of others with easy access to known vulnerabilities and threat tactics.

With fraud-as-a-service (FaaS), ransomware-as-a-service (RaaS), and phishing-as-a-service (PHaaS), savvy bad actors are profiting from what they know by enabling more amateurs. Historically, the biggest threats have come from organized fraud rings. Now, there will likely be a rise in amateur fraudsters and lone actors, increasing both the volume of attacks and the number of attacks that leverage sophisticated techniques.

Trends Snapshot

Biggest growing threats from 2024:

- Digital document manipulation
  - Digital document forgeries have increased 244% YoY
- Deepfakes
  - Deepfake attempts occurred at a rate of one every five minutes in 2024
  - Deepfakes account for 40% of all biometric fraud

Top 3 most targeted industries:

1. Cryptocurrency
2. Lending
3. Traditional banks

Most vulnerable document type:

- National ID cards

Most targeted document:

- India Tax ID

Region with the highest fraud rate:

- Asia

Region with the biggest increase in fraud:

- Americas

FRAUD TRENDS

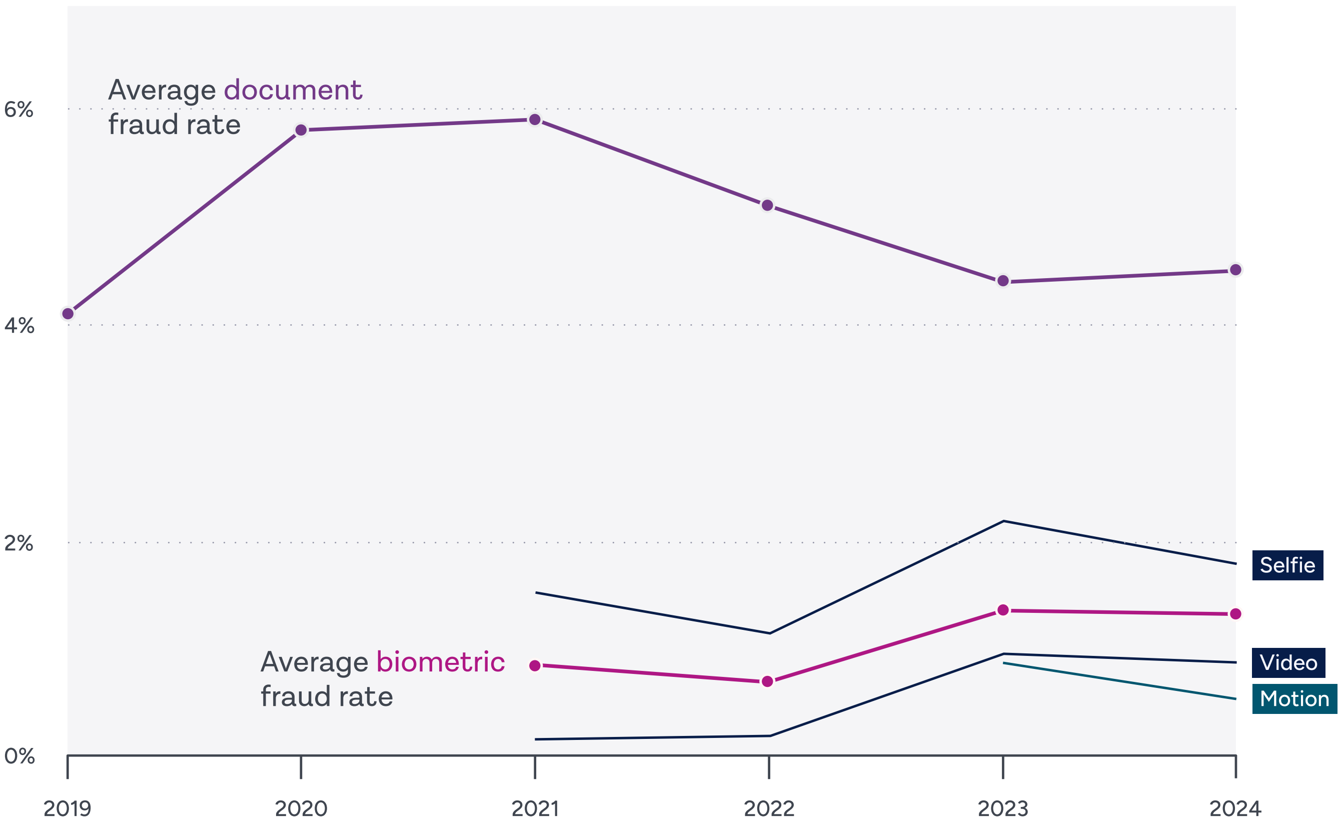
Data Stories

How Globalization, Digitization, and AI Are Reshaping Fraud

Average fraud rates help monitor for any significant changes in year-over-year fraud levels. Compared to last year, average fraud rates remained stable – document fraud rates are at 4.5%, and biometric fraud rates are at <2%. What is clear is that biometrics (and particularly biometrics that include a liveness element – video or motion, for example) continue to act as a stronger deterrent against fraud than just document alone.

This graph provides a snapshot into how fraud patterns have shifted and developed over time. There are three distinct periods that emerge out of these five years' worth of data, which are discussed in more detail on the next page.

Average fraud rates



Pre-COVID: 2019

Before the COVID-19 global pandemic, there were several distinct trends across fraudulent attacks. While the world was very much "online," many fraud techniques still relied on physical means. For example, most document fraud was performed on a physical identity document.

Certain sectors (like financial services) were also much more online than others. This likely correlated to higher fraud rates than those sectors who were lagging digitally – or at least until it became a necessity in 2020 and beyond. Fraudsters also didn't have the same level of connectivity as they have today, and fraudulent attacks mirrored the hours of an average working week, with most fraud attacks taking place Monday to Friday.

Peak pandemic: 2020-2021

During the pandemic, there was a marked uptick in fraud. Turbulent economic times tend to correlate with a rise in fraud, and the pandemic put huge economic strains on both businesses and individuals. This led to a rise in scams, with 75% of online merchants reporting an increase in fraud attempts after the beginning of the COVID-19 pandemic, according to Statista. And the Government Accountability Office estimated that between $100 billion and $135 billion in unemployment benefits were fraudulently obtained through funding meant for pandemic relief efforts.

There was also an increase in fraud linked to the explosion of availability of online services. Many businesses had to hastily implement digital onboarding processes, and fraudsters sought to take advantage of this. The rapid increase of online connectivity, services, and offerings also changed the frequency of attacks. Fraud attacks shifted from mirroring an average work week to happening 24/7. This period was also pre-GenAI, which meant the majority of fraud was high-volume but low-sophistication.

Post pandemic: 2022-2024

Following the pandemic, average fraud rates fell back to just above their pre-pandemic levels. During this period, the world opened back up and people returned to work, albeit with a stronger focus on work-from-home culture. With a permanent hybrid workforce, IT teams were challenged to secure resources without the benefit of a company perimeter. Adopting a Zero Trust strategy became paramount to maintaining workplace and workforce security, including the use of multi-factor authentication (MFA) and encryption. And as 2024 dawned, this identity-centric approach became AI-powered.

In the last few years, there has also been a rise in geopolitical tensions around the world. Associated economic sanctions are incenting some nation-state attackers to increase their reliance on fraud as a source of revenue to fund operations, as well as use fraud to help launder money – using cryptocurrency, for example. Simultaneously, inflation rates hit a 10-year high in 2023, placing increasing pressure on the cost of living, contributing to an increase in scams and financial fraud.

In recent years there has also been a marked shift in some of the tactics used by fraudsters. The availability and sophistication of online tools (GenAI in particular) are contributing to a rise in both the volume and sophistication of attacks – for example, an increase in digital document manipulation and deepfakes.

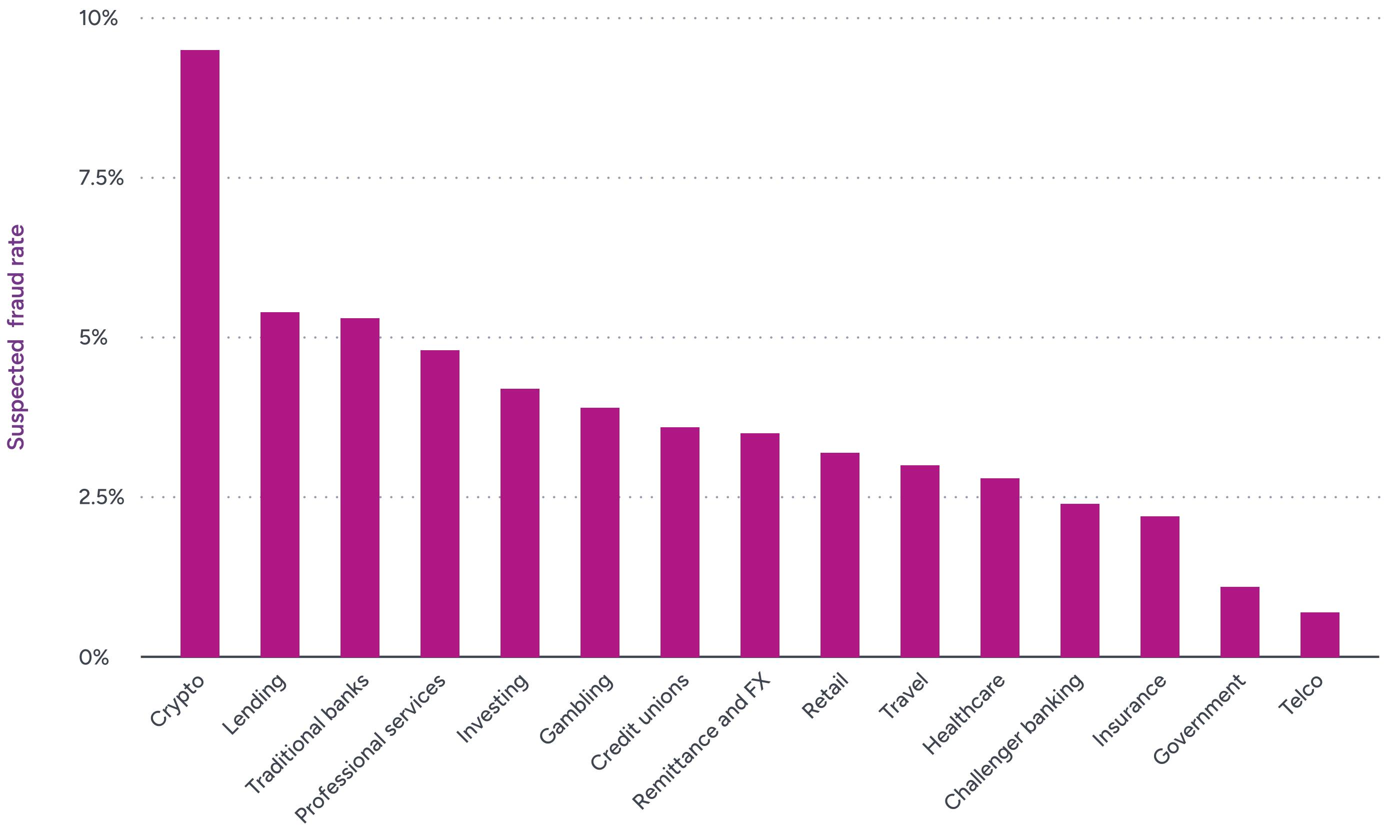
Industries Under Attack

Fraudsters focus on finance

The top three most targeted industries in 2024 were all financial services related, with cryptocurrency seeing almost double the amount of fraud attempts compared to any other industry, followed by lending and traditional banks.

It's worth noting that while some industries may see a higher volume of fraud attempts than others, it doesn't mean that fraudsters won't turn their attention elsewhere. Fraudsters tend to "rinse and repeat" their tactics. If they find a loophole to exploit across one area, they will then redeploy it and test other organizations' defenses.

Industry fraud rates

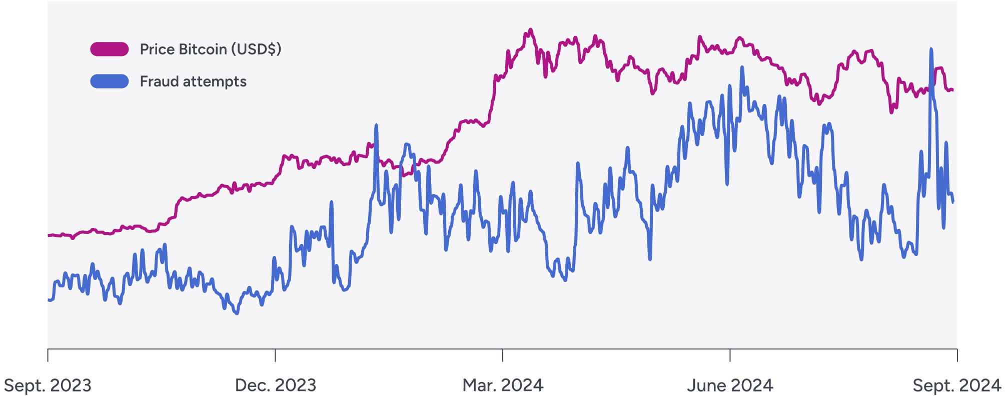


Cryptocurrency

An FBI report found that reported losses from cryptocurrency-related fraud in 2023 increased 45% compared to the previous year, exceeding $5.6 billion. These losses are mostly linked to investment-related scams, confirming that cryptocurrency remains a top target for fraudsters.

When it comes to customer onboarding, crypto platforms saw the highest rate of fraudulent attempts compared to any other industry. Fraudulent attempts are also up 50% year-over-year, from 6.4% in 2023 to 9.5% in 2024. This is unsurprising given that Bitcoin prices hit another all-time high in 2024, and it's estimated that there are now over 9,000 different cryptocurrencies worldwide. Where there is money and opportunity, there will always be fraud. We can see this in the chart below – as the price of Bitcoin rises, the number of fraud attempts typically do too.

With many eyes on the crypto space, more stringent regulation is likely to follow the European Union's example of the first comprehensive cryptocurrency regulations – Markets in Crypto-Assets Regulation (MiCA) – introduced in May 2023. And while more regulation can go some way to implementing better safeguards, individuals should remain wary of crypto investment promises that seem too good to be true, and they should take steps to research how and where they invest. The Financial Ombudsman Service, for example, has seen a significant rise in scam complaints where people handed over their money after seeing an investment opportunity on social media platforms.



Lending

For industries such as lending and mortgages where there are cash rewards on the table, there are always going to be fraud attempts. However, current market conditions with increased interest rates and costs of living are likely contributing to high rates of fraud, such as falsified applications and documents. More than ever, this highlights the need for vigilant verification processes when reviewing mortgage and loan applications.

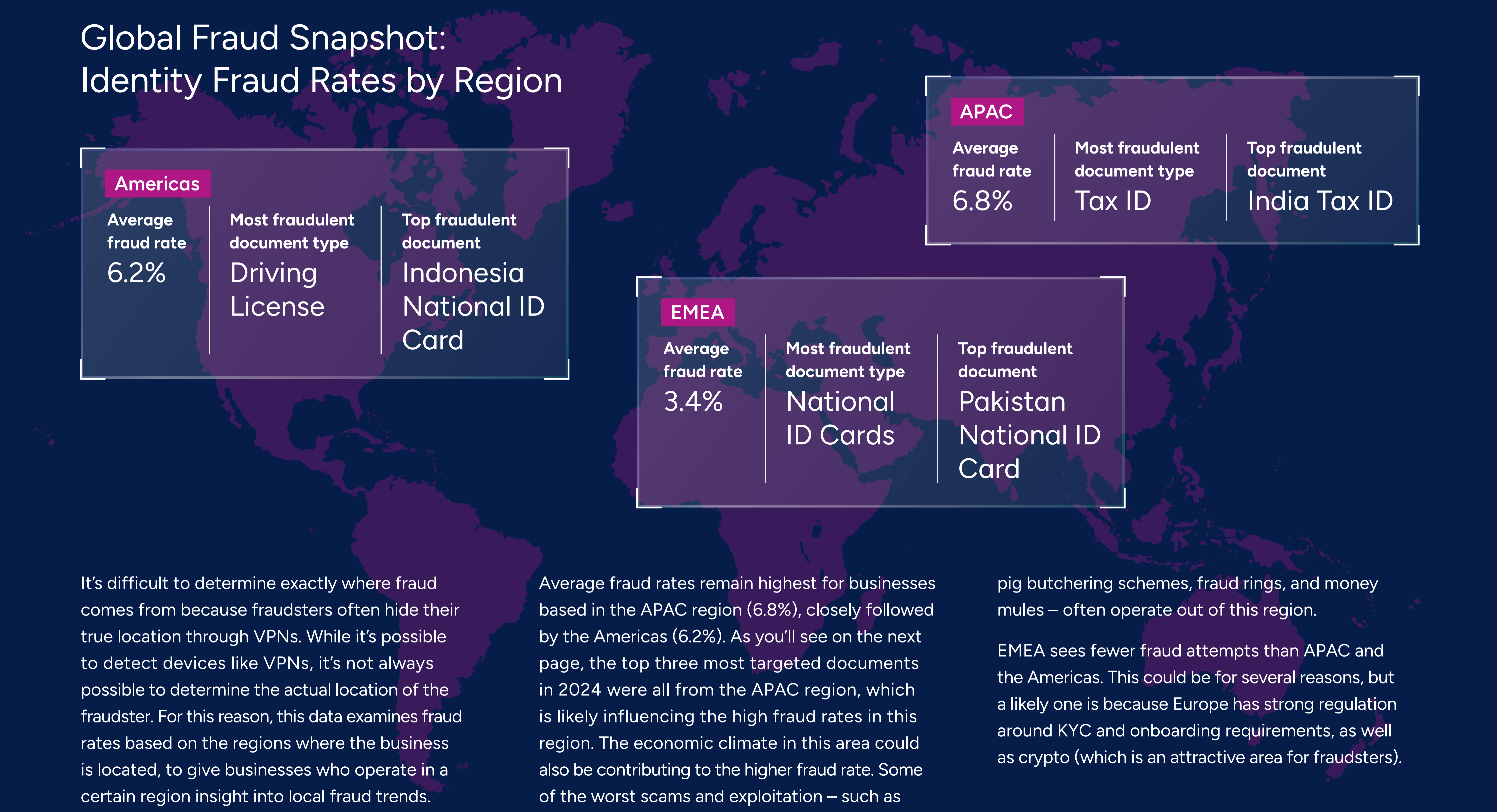
However, the current tough economic climate doesn't just put lenders and brokers at risk of fraud. Higher mortgage and lending rates can also lead to a rise in lending scams targeted at consumers. The Federal Trade Commission (FTC) reported nearly 26,000 cases of abuse of advance-fee loans last year, costing victims $75 million.

Traditional banks

Traditional banks are also seeing an increase in fraudulent onboarding attempts, which are up 13% from last year. Much like the lending and mortgages space, this is likely due to current economic conditions and the fact that bank accounts can unlock cash rewards for fraudsters, including more lending and credit opportunities.

Cybercriminals also have easier access than ever to AI tools, which adds to the threat of account takeovers at later moments in the customer lifecycle. Security experts have reported an 856% increase in malicious email and messaging threats over the previous 12 months. Bad actors are increasingly using GenAI tools to create convincing phishing emails – or for credential harvesting phishing attacks to try and gain unauthorized access to bank accounts and other financial accounts.

Global Fraud Snapshot: Identity Fraud Rates by Region



Americas

Average fraud rate	Most fraudulent document type	Top fraudulent document
6.2%	Driving License	Indonesia National ID Card

APAC

Average fraud rate	Most fraudulent document type	Top fraudulent document
6.8%	Tax ID	India Tax ID

EMEA

Average fraud rate	Most fraudulent document type	Top fraudulent document
3.4%	National ID Cards	Pakistan National ID Card

It's difficult to determine exactly where fraud comes from because fraudsters often hide their true location through VPNs. While it's possible to detect devices like VPNs, it's not always possible to determine the actual location of the fraudster. For this reason, this data examines fraud rates based on the regions where the business is located, to give businesses who operate in a certain region insight into local fraud trends.

Average fraud rates remain highest for businesses based in the APAC region (6.8%), closely followed by the Americas (6.2%). As you'll see on the next page, the top three most targeted documents in 2024 were all from the APAC region, which is likely influencing the high fraud rates in this region. The economic climate in this area could also be contributing to the higher fraud rate. Some of the worst scams and exploitation – such as pig butchering schemes, fraud rings, and money mules – often operate out of this region.

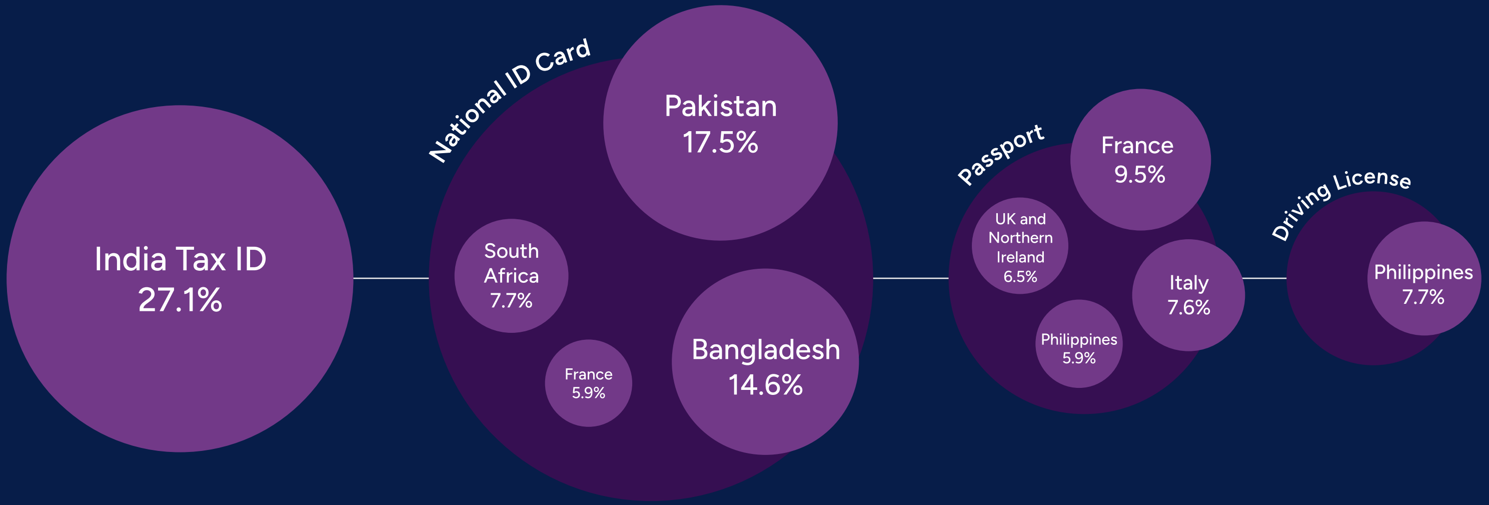
EMEA sees fewer fraud attempts than APAC and the Americas. This could be for several reasons, but a likely one is because Europe has strong regulation around KYC and onboarding requirements, as well as crypto (which is an attractive area for fraudsters).

Top 10 Most Targeted Documents

Some of the most targeted documents include the India tax ID, Pakistan national ID card, Bangladesh national ID card, and France passport.

The India tax ID is likely the most targeted document in 2024 because there are a lot of templates available online for this document. This makes it an easy target for digital manipulation (a document fraud technique that's skyrocketed this year – see page 17).

A lot of the national ID cards on this list (such as those in Pakistan, Bangladesh, and South Africa) still have older paper versions of the document in circulation. Paper versions are easier targets for fraudsters because it's easy to print out a version of the document at home.



Tax ID, India	27.1%		**National Identity Card**, South Africa	7.7%
National Identity Card, Pakistan	17.5%		**Passport**, Italy	7.6%
National Identity Card, Bangladesh	14.6%		**Passport**, UK and Northern Ireland	6.5%
Passport, France	9.5%		**Passport**, Philippines	5.9%
Driving License, Philippines	7.7%		**National Identity Card**, France	5.9%

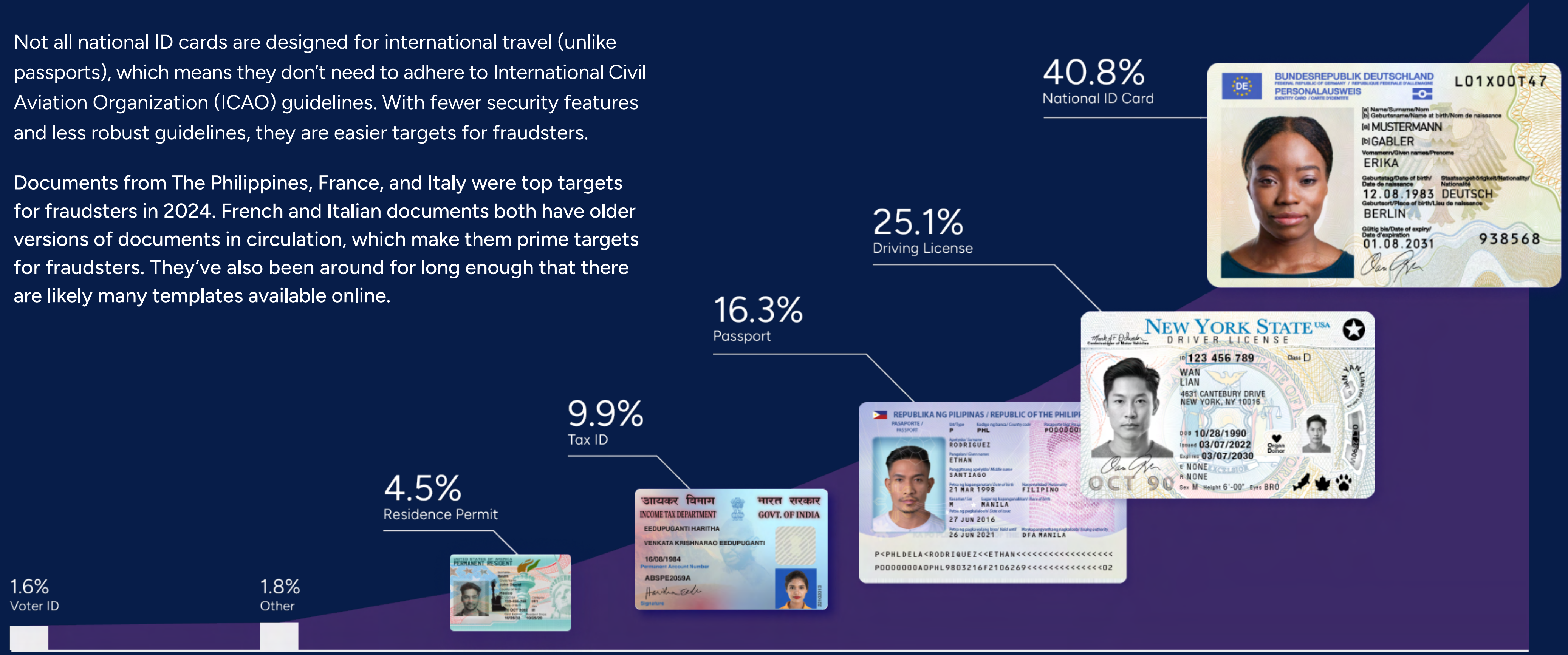
National ID Cards Remain Top Target for Fraudsters

Across all document fraud, 40.8% target national ID cards.

Not all national ID cards are designed for international travel (unlike passports), which means they don't need to adhere to International Civil Aviation Organization (ICAO) guidelines. With fewer security features and less robust guidelines, they are easier targets for fraudsters.

Documents from The Philippines, France, and Italy were top targets for fraudsters in 2024. French and Italian documents both have older versions of documents in circulation, which make them prime targets for fraudsters. They've also been around for long enough that there are likely many templates available online.

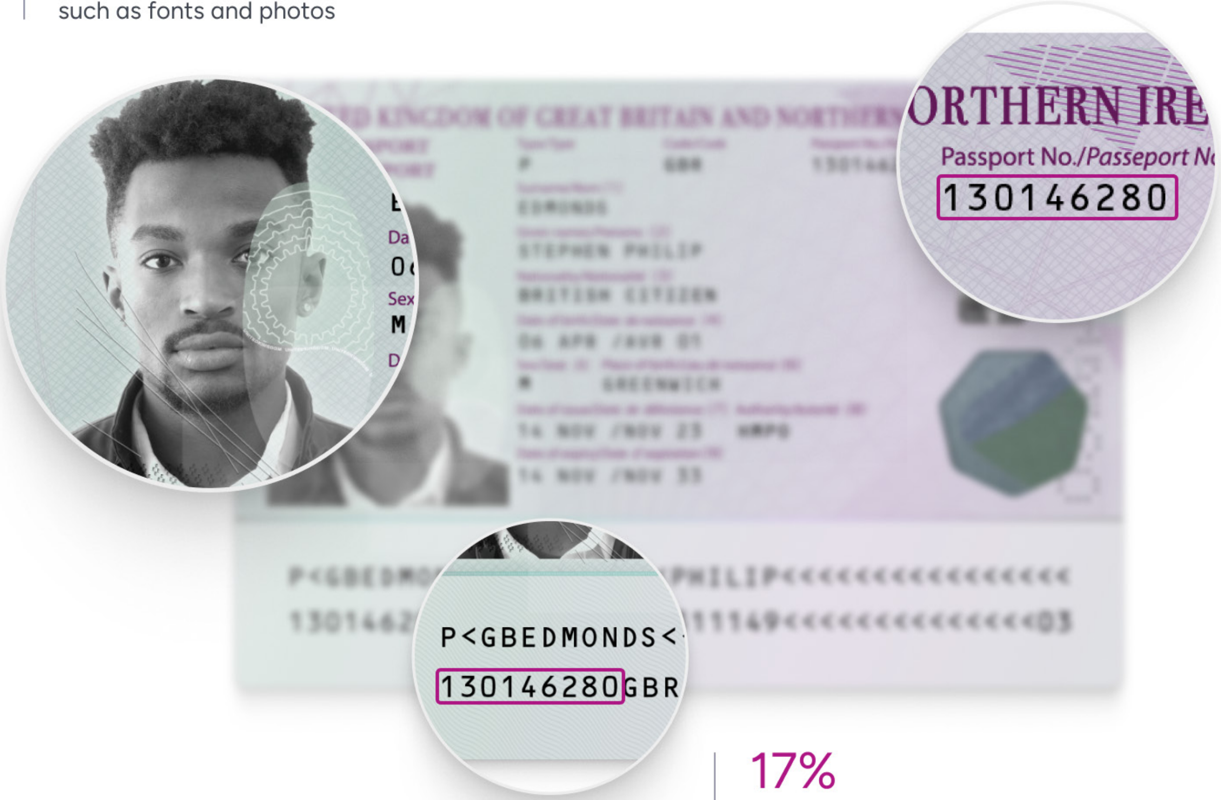
Fraud by document type



Key Indicators of Fraudulent Documents

Not all documents are created equal. As mentioned, certain document types (like national ID cards) simply don't need to meet as stringent guidelines as other document types. When verifying documents, this means it's necessary to use a variety of approaches to check for fraud. Especially given the prevalence of synthetic identity fraud, where fraudsters combine real and fake information to create a new identity. Verifying a document's authenticity can include examining both the data and visual security features on that document.

The majority of documents are flagged for either visual authenticity (47%) or data validation (36%), which points to more sophisticated attacks. However, simply checking that the data is consistent within the document can help catch large amounts of obvious fraud.



47%

Visual Authenticity

Check visual security features such as fonts and photos

36%

Data Validation

Check that a document has valid data in all the correct places

17%

Data Consistency

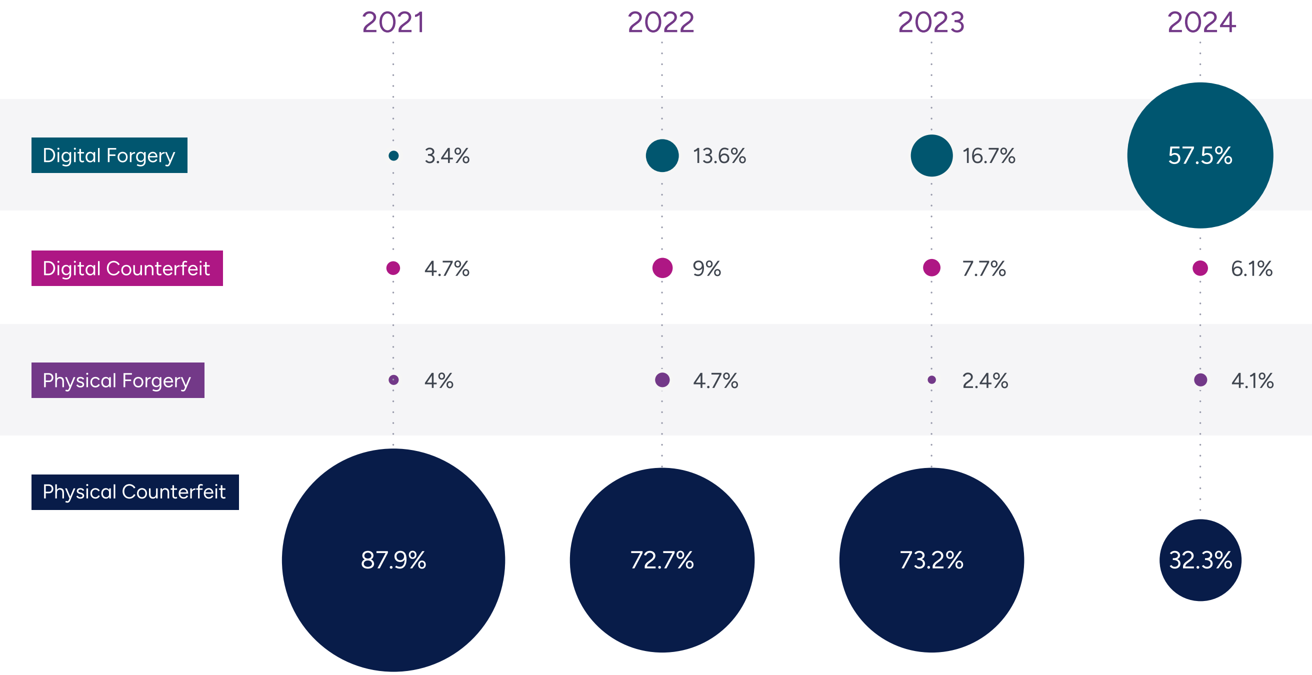
Check that data is consistent across all areas of a document where it's repeated

DEEP DIVE

Fraudster Techniques

GenAI Fuels Rise in Digital Document Fraud

How fraudsters target documents



Digital Forgery

Physical Counterfeit

There are two different types of fraudulent documents:

- ✓ **Counterfeits:** A complete reproduction of an identity document
- ✓ **Forgeries:** An altered version of an original document

And fraudsters manipulate these documents using one of two techniques:

- ✓ **Physical:** Making edits to or reproducing the actual physical document
- ✓ **Digital:** Manipulating a digital version of the document

Historically, fraudsters have predominantly created physical counterfeits for use in person, or even when targeting online customer onboarding. They would create the new physical document from scratch, then take a photo of it and submit it as part of the onboarding process.

However, the digital-to-physical ratio across document fraud has now shifted. For the first time ever, fraudsters are creating more digital forgeries than physical counterfeits, with digital forgeries accounting for 57.46% of all document fraud. That's a 244% increase over last year (when digital forgeries only accounted for 16.7%) and a 1,600% increase compared to 2021 when nearly all fraudulent documents were physical counterfeits.

This is a trend that's been brought about by the availability of AI-assisted tools, shared methodologies, and the rise of fraud-as-a-service. This type of technique is also much easier to scale because digital forgeries are easier and cheaper to produce than physical counterfeits, which require a manual printing process.

To create digital forgeries, fraudsters are accessing document templates online or downloading images of documents obtained via a data breach and manipulating the details in Photoshop. GenAI tools are speeding up this process, helping fraudsters produce more of these digital synthetic identities – cheaply and at scale.

Digital document forgeries are one example where we see fraudsters employing multiple tactics at once. Fraudsters with the know-how can profit from their knowledge by sharing methodologies across fraud-as-a-service platforms. These platforms provide information on how to manipulate documents, as well as the GenAI tools to help create digital forgeries. Then fraudsters use injection attacks (more on page 23) as the primary method to get digital forgeries into verification systems.

Deepfakes: The New Face of Video Biometric Fraud

Fraudsters use several techniques to target a biometric check. These differ depending on whether the biometric check involves a static photo (selfie) or a video element (video/motion).

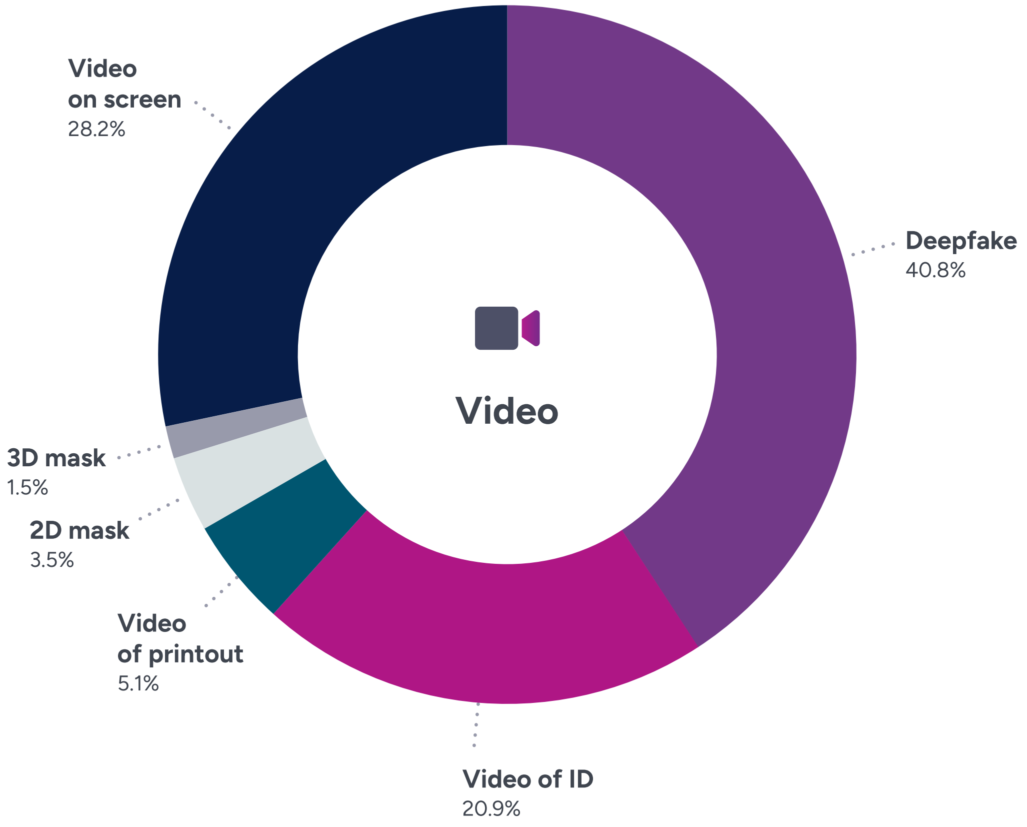


Photo on screen (selfie only): A photo of an image on screen (such as a profile picture from a social media account)

Photo of printout (selfie only): A photo of an image printed on paper

Photo/Video of ID: A photo or video of the face on the identity document

2D mask: A photo or video of a 2D-printed mask

3D mask: A photo or video of a 3D mask or other 3D object

Deepfake: Digitally manipulated photo or video where a person's face is altered to appear as someone else

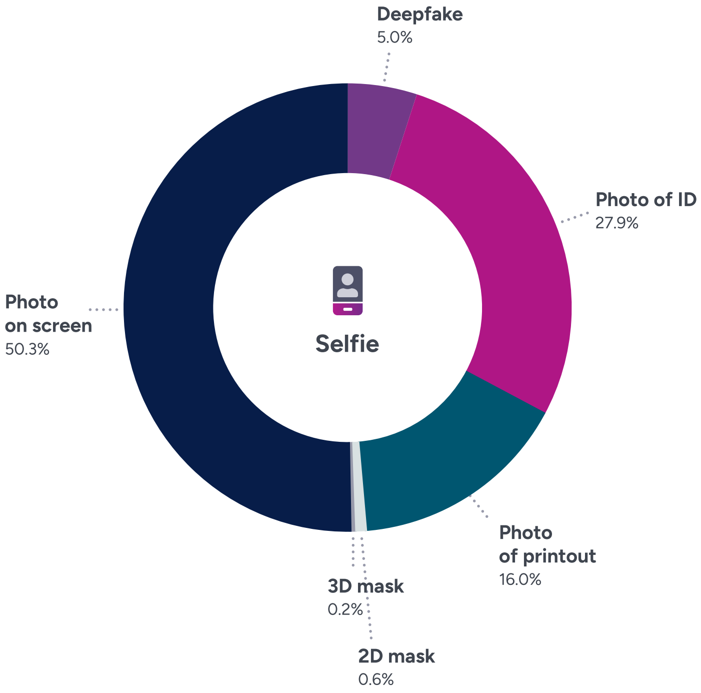
Video on screen (video/motion only): A video of a video on a screen

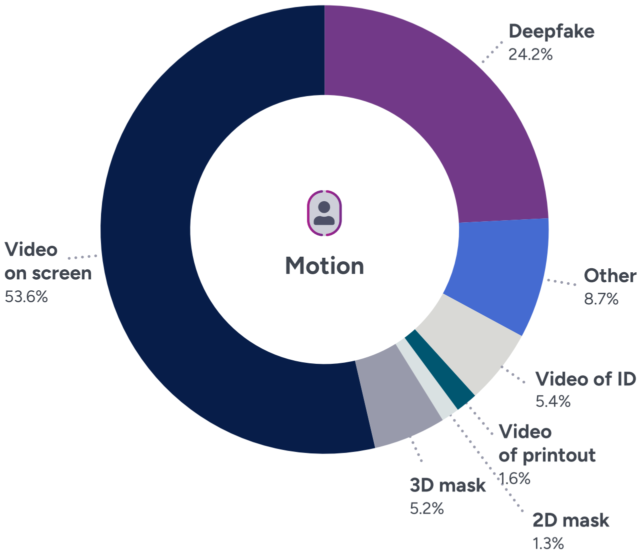
Video of printout (video/motion only): A video of an image printed on paper

There are different types of biometric checks. Capturing a selfie offers a passive solution to customers, whereas a video or motion verification involves a form of active liveness requiring the user to engage in a task. The different capture experiences result in different types of attacks, with differing levels of fraud sophistication across these solutions. Selfie-based solutions see more basic forms of attacks, such as photo on screens, which accounted for the most (50.29%) fraudulent attempts across selfies in 2024.

Comparatively, biometric checks that include an active liveness element see more advanced attacks because they are harder to bypass. They raise the barrier of entry for fraud by enforcing a live capture, meaning fraudsters must resort to more sophisticated methods of attack, such as deepfakes, to impersonate someone. This is why deepfakes make up such a large percentage (40.80%) of fraud attempts across video biometrics.

However, active liveness solutions are more robust against these types of attacks. They can analyze multiple frames to better detect anomalies that arise from deepfakes. Organizations that incorporate a liveness biometric check into their defenses are better protected not only against lower-sophistication fraud that can easily be performed at scale, but also against rapidly evolving deepfake technologies – for a holistic protection against fraud.





Product highlight

With deepfakes becoming more realistic and harder to spot (even for trained experts), it has become more effective to fight AI with AI. Compared to humans, AI is better at detecting sophisticated attack vectors like deepfakes.

Motion Biometric Verification is 100% AI driven, powered by anti-spoofing models that are specifically trained to catch deepfakes. Businesses that are serious about preventing deepfakes should consider incorporating fully automated systems such as Motion into their defenses.

The Impact of Deepfakes

The prevalence of face-swap apps and GenAI tools have made it increasingly accessible and scalable for fraudsters and cybercriminals to create deepfakes. Their capacity for malicious usage is widespread, and includes:

- ✓ **Fraudulent account opening:** Using deepfakes to bypass identity verification during a KYC onboarding process and open fraudulent accounts
- ✓ **Phishing/Investment scams:** Leveraging deepfake technology to create fake videos (such as of a celebrity endorsing a new investment opportunity, or a company executive asking employees for favors) and convincing people to hand over money or personal data
- ✓ **Account takeover:** Using deepfakes to dupe biometric checks and gain unauthorized access to existing accounts
- ✓ **Political or misinformation campaigns:** By impersonating public or political figures, cybercriminals can use deepfake images and videos to spread misinformation, or even to try to influence election outcomes

What are deepfakes?

Deepfakes are digitally manipulated videos or images where a person's face is altered to appear as someone else. They vary in sophistication and fall into one of two categories:

1. **Face swaps:** Where a new face is superimposed onto a target head. The most basic method, where one face is crudely pasted over another face, results in a "cheapfake." Sophisticated face swaps use AI to morph and blend a new face onto the target.

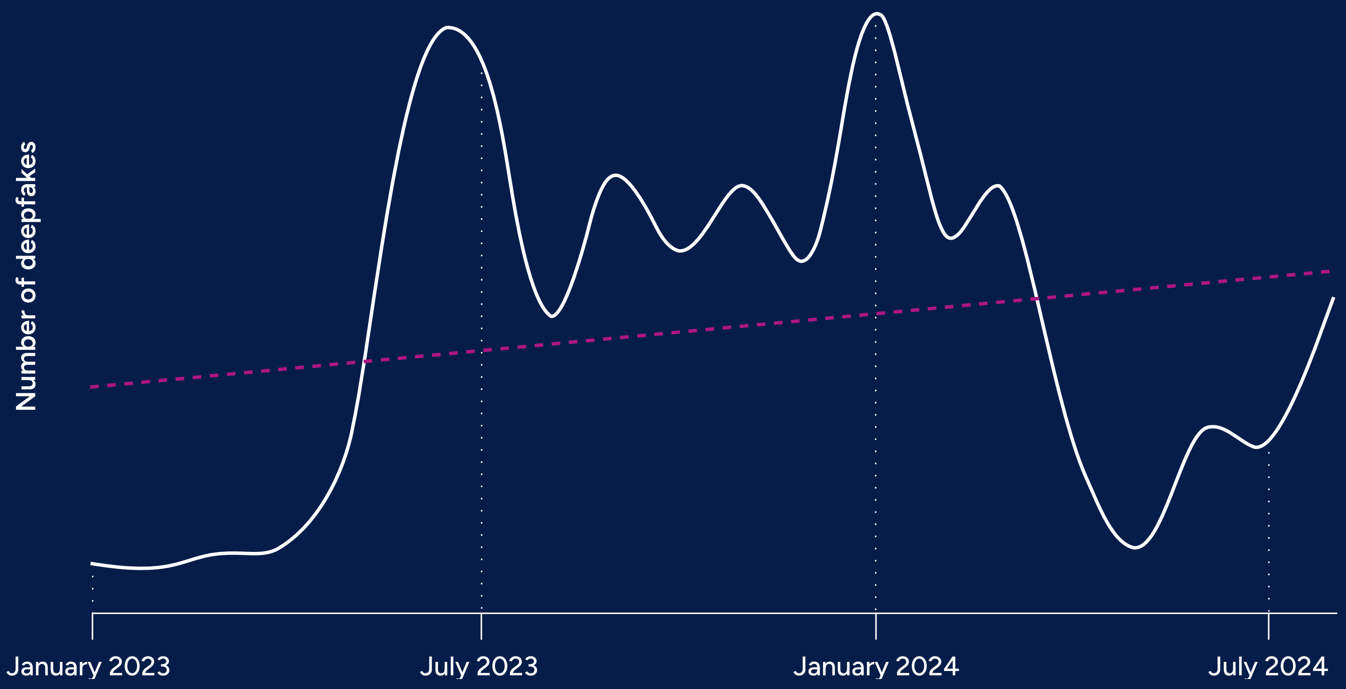
2. **Fully generated images:** These are created by generative models that have been trained to produce extremely realistic images and videos of faces.

2023 was the first year that deepfakes became a widespread attack vector, and they have continued to pose a significant threat to businesses throughout 2024.

Between 2022 and 2023, the number of deepfakes increased 3,000%, with volumes peaking in June 2023. In January 2024, deepfake volumes reached another all-time high, and volumes continue to fluctuate throughout 2024 as IDV vendors introduce new detection technologies, prompting swift adaptations by fraudsters in response. Overall volumes, however, are trending up, and in the last 12 months, there has been, on average, one deepfake attempt every five minutes.

A 2024 Deloitte survey also found that deepfake financial fraud is expected to surge in the next 12 months. According to the survey, more than half of C-suite executives and other senior leaders anticipate a rise in both the frequency and scale of deepfake attacks targeting their companies' financial and accounting data.

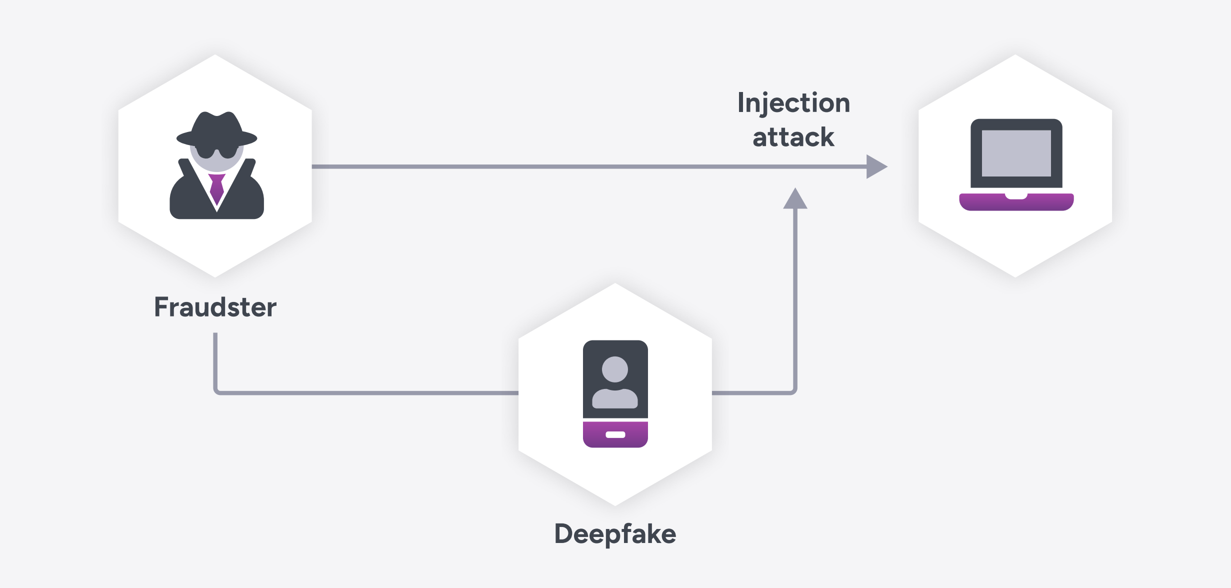
Financial services are a prime target for deepfakes. Historically, they have stringent fraud-prevention techniques, which means fraudsters are likely to turn to more sophisticated attack vectors like deepfakes to reap large cash rewards. Criminals are using AI to create convincing fake documents, emails, and even deepfakes, in their attempts to authorize fraudulent transactions.



Injection Attacks and Their Role in Deepfake Submission

One of the main ways that fraudsters are submitting deepfakes is via a technique known as injection attacks. The purpose of an injection attack is to manipulate video or photo feeds to bypass the usual onboarding capture process and introduce a false identity into the system. This makes them of particular concern for businesses who verify customer identities as part of their KYC onboarding obligations.

Identity verification processes typically involve a live capture experience where an individual takes a photo of their identity document and a biometric signature (usually their face) in real time. Injection attacks are a form of cyberattack where the fraudster compromises the integrity of that system by inserting fake content (usually a deepfake) into the data stream.



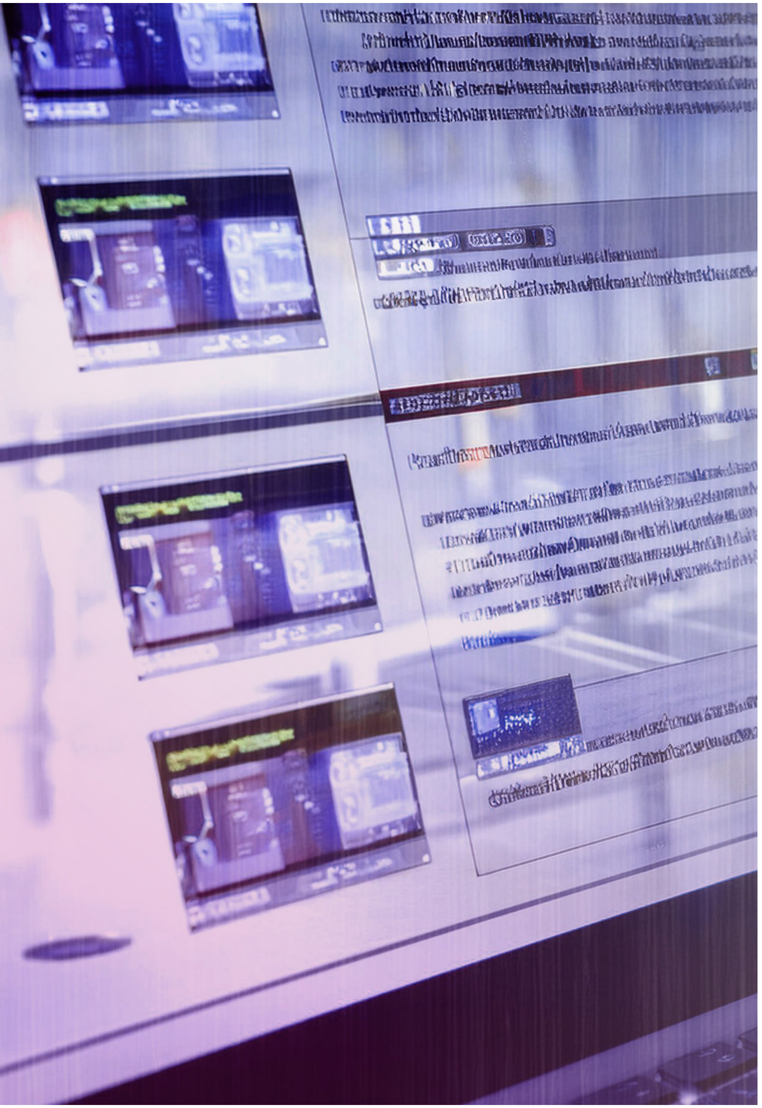
Different types of injection attacks

- **Virtual cameras:** This is the most common method fraudsters use for injection attacks. They replace a real hardware camera with software, allowing them to use any source video or recording.
- **Network injection:** This less common but more sophisticated type of attack requires technical knowledge, where fraudsters use code to submit deepfakes.

Preventing injection attacks

Preventing injection attacks requires a multi-layered approach:

1. **At the source (video input):** Leveraging background signals to check for suspicious activity or specific patterns linked to the media or device submitting the check
2. **At presentation (video content):** Enforcing real-time biometric capture experiences that require some form of dynamic interaction, and analyzing that video content to detect anomalies or inconsistencies in the facial movement
3. **At submission (cross-comparing):** Leveraging AI systems and machine learning (ML) to detect deepfakes once the deepfake has made its way into the back end



Fraud-as-a-Service (FaaS) and Shared Methodologies

Fraud-as-a-service (FaaS) is the practice of outsourcing or sharing information and services to others, often for a fee.

Such information and services (found mainly via the dark web) include things like hacking tutorials, playbooks, and cybercrime courses, as well as access to stolen PII such as login credentials, Social Security numbers, and credit card information. According to a 2023 study, cybercriminals could purchase the details of a credit card with a $5,000 balance for around $110 (USD).

Given that most of this activity happens on the dark web, it's incredibly difficult to measure the scale and impact of it. But fraud-as-a-service will continue to grow as a threat for two reasons.

1. GenAI tools such as ChatGPT (and clones designed specifically for malicious purposes, such as WormGPT) have contributed to the rise of FaaS, as it's become much easier for fraudsters to generate things like email templates at scale. These tools aren't going anywhere and will only become more accessible and sophisticated as time goes on.
2. It lowers the barrier to entry for both potential fraudsters and increasingly sophisticated fraud vectors. Historically, only a small number of fraudsters – often professional fraud rings – had access to the information and tools to conduct sophisticated fraud. But by sharing and profiting from this information, they're now making it easier for amateur fraudsters to enter the game.

Synthetic Identities: From Stolen SSNs to Fake IDs

As tools and technology have become more powerful and readily available for fraudsters, the creation of synthetic identities could skyrocket.

The difference between traditional identity fraud and synthetic fraud is that with **traditional identity fraud**, a bad actor steals an individual's personally identifiable information (PII) and misuses it by falsely representing themselves as the person's actual identity. With **synthetic identity fraud**, a bad actor creates a completely new identity by combining real and fake PII, such as date of birth (DOB), name, and Social Security number (SSN) to create a new, completely fabricated identity.

The fact that digital document manipulation has increased 244% since last year is an indicator of the types of techniques fraudsters are leaning into to create synthetic identities. The availability of things like fraud-as-a-service, GenAI tools, and online templates means it's incredibly easy for fraudsters to get their hands on stolen PII or to create fabricated identities at scale – without ever even touching a physical document.

All of this is contributing to making synthetic identity fraud one of the fastest-growing financial crimes. The Deloitte Center for Financial Services estimated that in the U.S. alone, synthetic identity fraud will generate at least $23 billion in losses by 2030. Synthetic identities continue to pose a significant threat because they persist. If they aren't identified at day one, they can remain in an organization's system over time, slowly building a credit score before maxing out to reap the reward.

Methods that fraudsters use to create synthetic identities include:

- **Identity manipulation:** Authentic PII elements are adjusted slightly to create a new fake identity
  Example: the alteration of an attribute such as changing the date of birth or a name on a driver's license
- **Identity compilation:** Actual and fabricated PII data elements are compiled together to form a new identity
  Example: associating a real SSN with a completely fabricated identity document
- **Identity fabrication:** A new fake identity is created without the use of any genuine PII
  Example: the creation of a completely fictitious identity without the inclusion of any personally identifiable information attributes, such as an identity document template populated with all fabricated information, combined with a deepfake

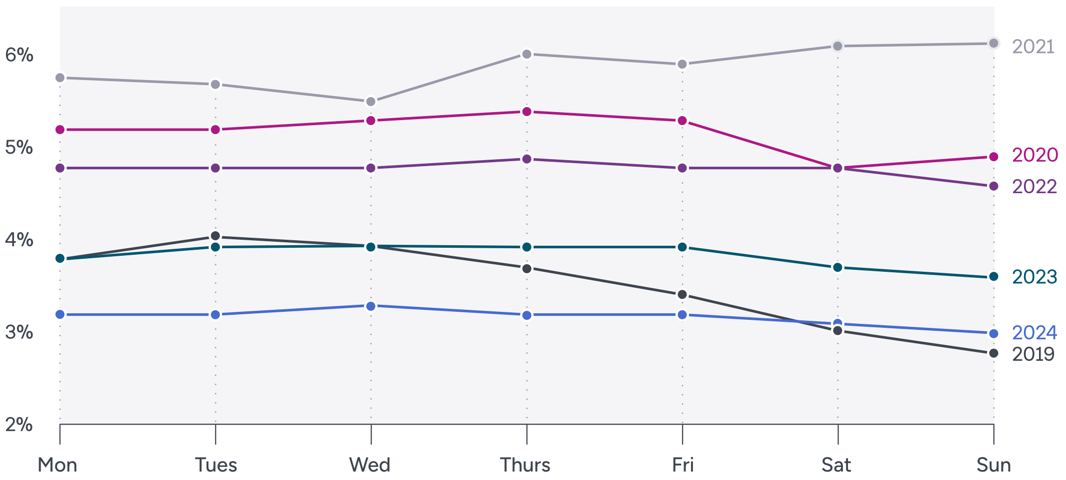
Globalization and the Rise of Coordinated Fraud Attacks

Communications, payments, and services transcend borders. And so does fraud. It happens anytime, anywhere, and to anyone. The interconnectivity of services has made it easier for fraud and other cyberattacks to circumvent borders, time zones, and other barriers.

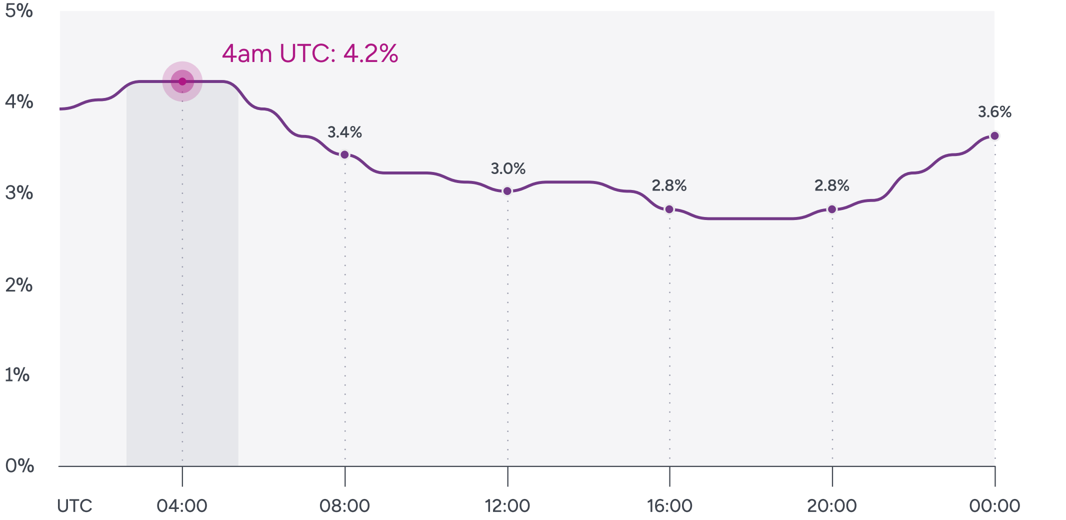
Fraud happens 24/7

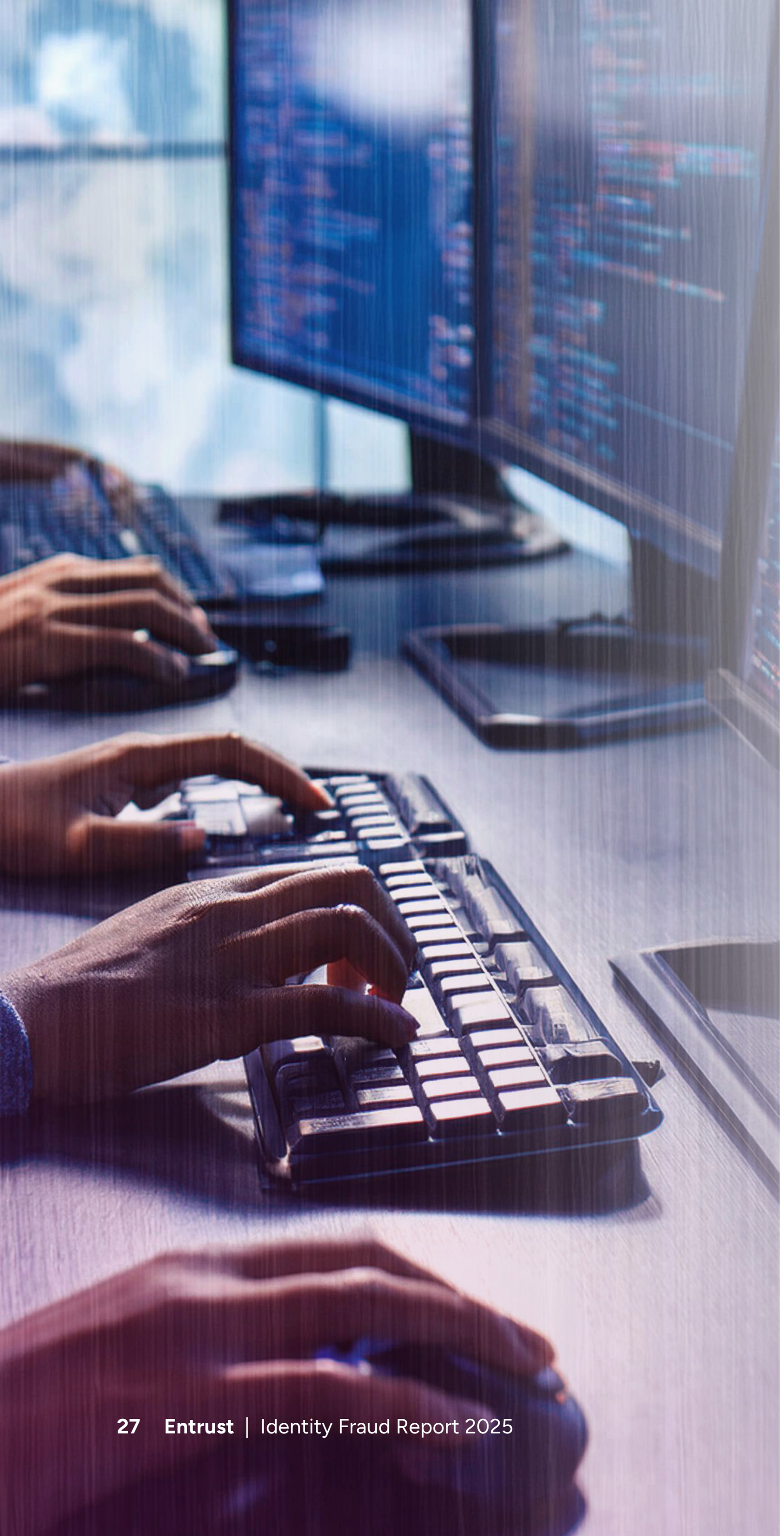
The data shows that fraud happens consistently 24 hours a day (with the exception of a small spike between the hours of 3 and 6 am UTC), seven days a week. The key takeaway: Fraud can happen at any time. In fact, fraudsters may even try to take advantage of what they assume to be business "downtime" hours – for example, during the early hours of the morning. In response, business defenses need to operate fraud-prevention tactics around the clock.

Average fraud rates by day of the week



Average fraud rates by time of day



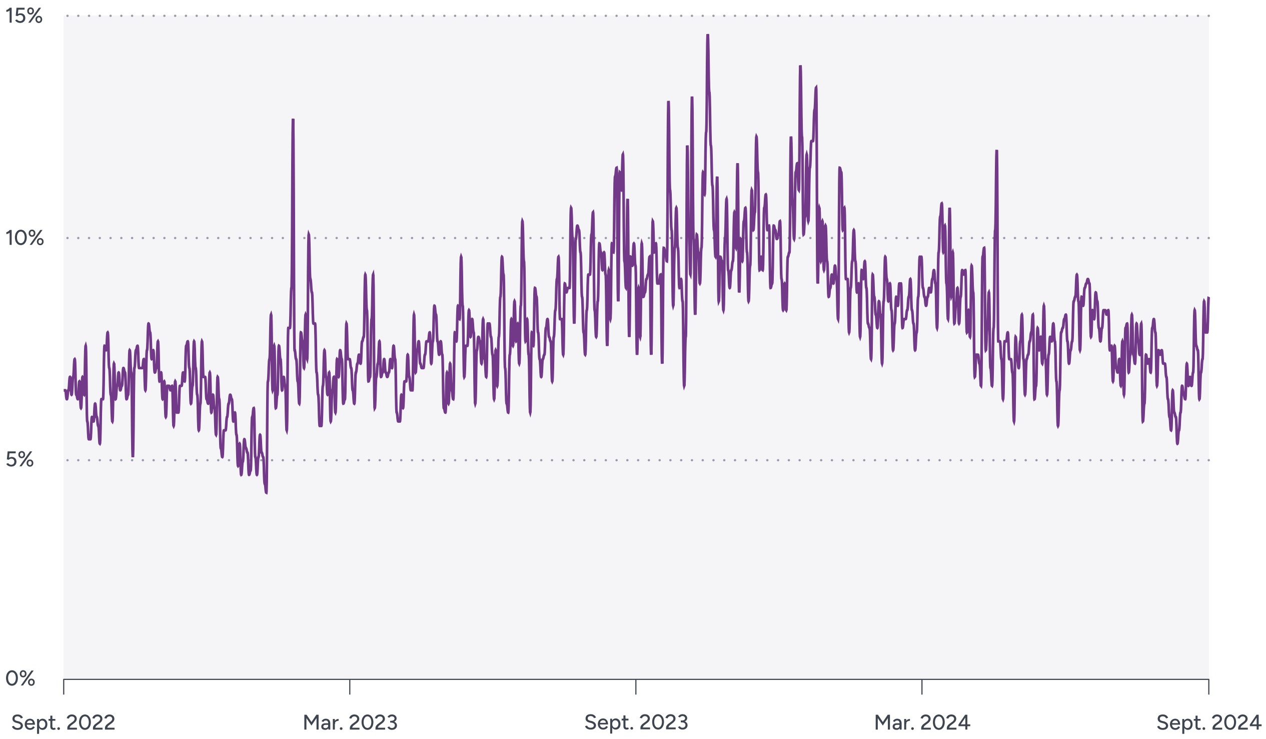


Fraudsters Focus Their Efforts

Fraudsters tend to rinse and repeat their tactics. This graph shows average fraud levels across each day of the year. While some spikes might be linked to certain geopolitical events, or certain seasonality changes (such as holiday periods where spending is higher), the spikes could also represent coordinated attacks aimed at one business, or a small group of businesses.

These types of coordinated attacks are closely associated with organized fraud rings that have the resources and means available to launch such large attacks, at scale.

Average fraud rates by day of the year



LOOKING AHEAD

Identity Fraud in 2025

1. The increasing use of AI

AI-assisted tools have already had a sweeping impact across fraud. This is unlikely to change heading into 2025. Such tools will continue to increase both the volume and sophistication of fraud and other cybersecurity scams.

There has been a big focus on GenAI and how fraudsters are leveraging it to create new media to their advantage. This includes:

- **Deepfake creation:** Using face-swap apps and other software available online to create realistic deepfakes to attempt to open fraudulent accounts or gain unauthorized access to existing accounts
- **Voice spoofing:** Creating new or replicating voices of other individuals – for example, to bypass vocal recognition software
- **Generating text and image content:** GenAI tools, such as ChatGPT, DALL-E, and Midjourney, are making it easier to create text and image content, such as phishing email templates, from scratch
- **Data scraping:** Automating the scraping and collecting of enormous amounts of data for use in synthetic identity creation or credential stuffing
- **Bots:** For credential stuffing (where bots use stolen account credentials to gain unauthorized access to user accounts) or to automate the submission of loan or credit card applications using stolen or synthetic identities

One of the key challenges when it comes to AI and fraud is that it's hard to determine which cases involved AI. This makes it difficult to grasp the full scale of the problem and measure the threat. We can measure the impact in some areas (for example, we know that deepfakes are increasingly impacting customer onboarding). But in other areas, such as social engineering and phishing scams, it's a lot harder. For example, according to SlashNext's The State of Phishing 2024 report, there has been a 4,151% surge in malicious phishing messages since the launch of ChatGPT in November 2022, but it's difficult to determine how many of these actually involved AI-generated content.

However, while there are plenty of examples of AI for "bad," there are also many instances where businesses can use AI for "good," to their own advantage. While a lot of AI-related fraud involves GenAI, businesses are increasingly leveraging applied AI (AI designed to solve a particular problem) in their own fraud-prevention solutions.

2. AI (specifically deepfake) regulation

The regulatory landscape surrounding AI is particularly complex. For one thing, there are many different types of AI. For another, most uses of AI are not for malicious purposes. Any regulation, therefore, must strike a balance between protection and safeguards, while supporting innovation. Finally, AI regulations also differ depending on geographic location, with different regulators taking different approaches.

However, given the current focus on AI (and particular on its ability to cause harm) we're likely to see more proposals and frameworks around AI in 2025.

Current approaches to regulation

The U.S.

Currently, there's no comprehensive federal legislation or regulation that regulates the development of AI or prohibits or restricts any specific uses. However, there are some existing frameworks and guidelines, such as:

- The White House Executive Order on AI (titled Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence)
- The White House Blueprint for an AI Bill of Rights

There's also currently no federal law in the U.S. that prohibits the sharing or creation of deepfake images, but there is a growing push for this to change. Proposed regulation includes:

- The No Artificial Intelligence Fake Replicas And Unauthorized Duplications (No AI FRAUD) Act
- The Senate's Nurture Originals, Foster Art, and Keep Entertainment Safe (NO FAKES) Act
- The Disrupt Explicit Forged Images and Non-Consensual Edits (DEFIANCE) Act

Some individual U.S. states have already implemented or are in the process of implementing deepfake legislation. However, the current laws vary state by state. Some states with more comprehensive legislation that specifically targets deepfake content include California and Texas. The California Deepfake Law is at the forefront of AI regulation in the U.S. It was one of the first in the country to take effect back in 2019. The legislation not only criminalized non-consensual deepfake pornography but also gives victims the right to sue those who create images using their likenesses (Assembly Bill 602) and bans the use of AI deepfakes during election campaign season (Assembly Bill 730).

Texas was one of the first states in the country to pass a law prohibiting the creation and distribution of videos intended to harm or influence elections (Texas Senate Bill 751). Since then, the Texas Deepfake Law has introduced the Unlawful Production Or Distribution Of Certain Sexually Explicit Videos law, making it a criminal offense to produce explicit deepfake videos without the depicted person's permission.

Other states with legislation that targets deepfake content include Florida, Georgia, Hawaii, Illinois, Minnesota, New York, South Dakota, Tennessee, Texas, and Virginia.

Europe

The EU AI Act is currently the world's most comprehensive AI law, and similar to GDPR, will likely set the gold standard for AI regulatory efforts around the globe. It entered into force across all 27 EU Member States on August 1, 2024, and the enforcement for most of its provisions will commence on August 2, 2026.

The Act assigns applications of AI to three risk categories.

1. **Unacceptable risk:** Applications and systems that create an unacceptable risk are banned, such as cognitive behavioral manipulation and social scoring
2. **High-risk applications:** These applications are subject to specific legal requirements and include things like AI systems that are used in certain products or AI systems that fall into specific areas
3. **Applications not explicitly banned or listed as high-risk:** These are largely left unregulated but may be subject to transparency or copyright laws

When it comes to deepfake regulation, the Act does not bar the use of deepfakes outright but attempts to regulate them through transparency obligations placed on the creators under Article 52(3) of the Act.

The UK

In early 2024, the UK government unveiled its response to the AI Regulation White Paper published in August 2023. The government is proposing a "pro-innovation" approach, spearheaded by the Department for Science, Innovation and Technology (DSIT).

While the UK does not currently have AI-specific regulation in place, the government proposes a "principles-based framework" for regulating AI underpinned by five core principles:

- Safety, security, and robustness
- Appropriate transparency and explainability
- Fairness
- Accountability and governance
- Contestability and redress

The UK government's Office for Artificial Intelligence, which was set up to oversee the implementation of the UK's National AI Strategy, will perform various central functions to support the framework's implementation.

Regarding deepfakes, the UK Online Safety Act passed in 2023 has made it illegal to share explicit images or videos that have been digitally manipulated. However, this only applies in specific circumstances.

3. Data security and Zero Trust

The global average cost of a data breach reached an all-time-high of $4.88 million in 2024, a 10% increase from 2023, according to an IBM report. Data breaches are not new – it seems barely a day passes without another data breach reported in the news. Data breaches and fraud go hand-in-hand, because the more compromised data there is, the more PII fraudsters have access to. And the more PII they have access to, the more identity fraud they're able to commit. And this makes adopting a Zero Trust strategy with its core "Never Trust, Always Verify" principle and the associated use of identity-centric solutions an absolute must. This includes the application of AI-powered biometric identity verification, identity and access management (IAM) best practices like MFA, and digital signing to create trusted identities at day one (onboarding) and maintaining them to day two, three, and beyond.

4. Preparing for the post-quantum era

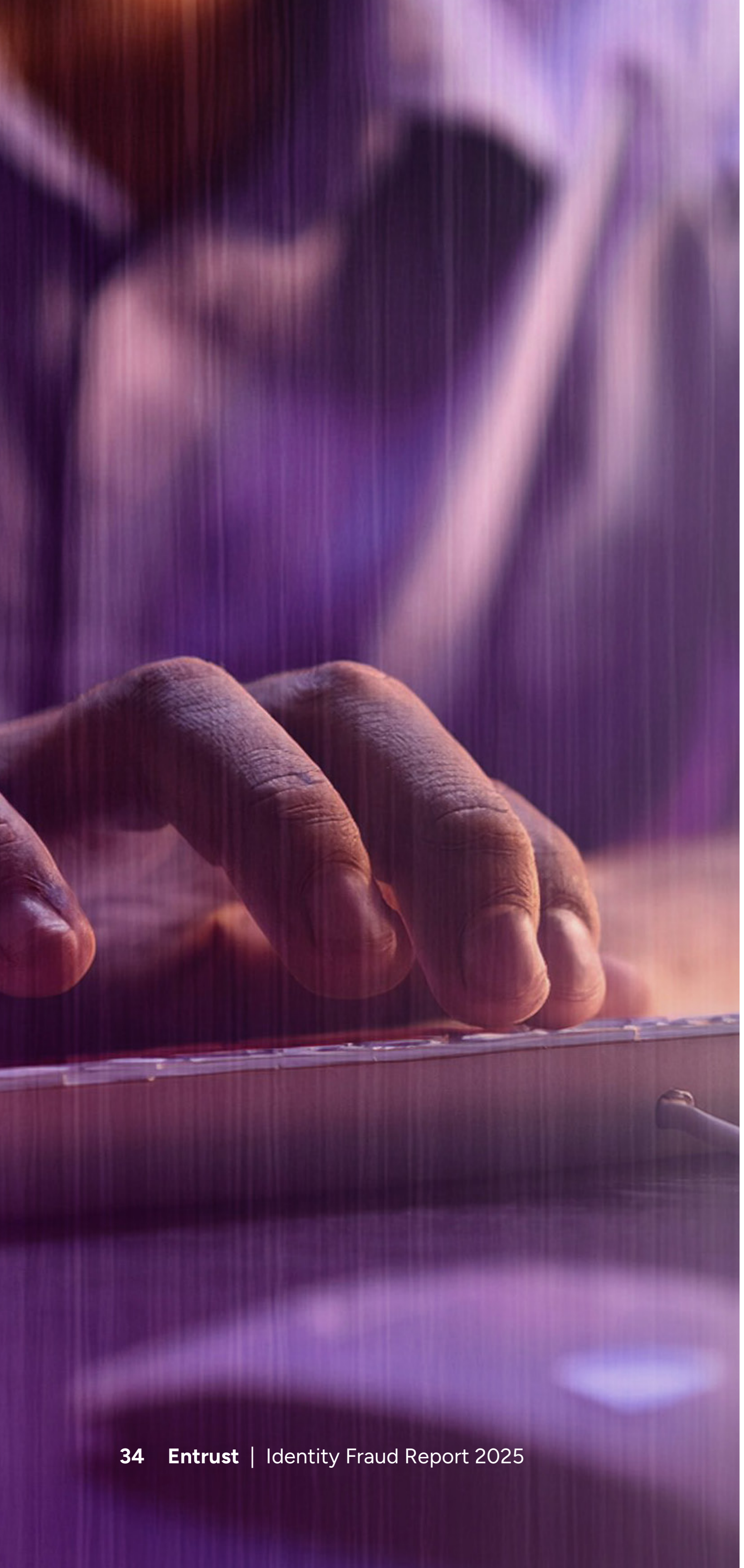
By 2029, the global cost of cybercrime is estimated to reach $15.63 trillion. And while that's a scary figure, what's perhaps scarier is that as quantum computing continues to mature, we're moving closer and closer to cryptographically relevant quantum computers (CRQCs). CRQCs will break the conventional encryption we rely on today to help keep users and data secure, ushering in the post-quantum (PQ) era. Yet in many ways, the PQ era and associated cyber threat is already here with "Harvest Now, Decrypt Later" style attacks that target long-life data like financial records and government intelligence. In recognition of this risk, NIST issued the first post-quantum cryptography (PQC) standards in August 2024 to help organizations navigate the journey to PQ. The good news is that, according to Entrust's 2024 State of Zero Trust & Encryption Study, 61% of IT and IT security practitioners report that their organizations are planning to migrate to PQC within the next five years.

5. eIDs and digital identity wallets

The idea behind electronic IDs (eIDs) is that they carry the same legal weight as a physical identity document. eIDs are intended to be interoperable across a wide range of legal, organizational, and technical systems. The European Digital Identity Regulation, for example, aims to create a system for EU citizens to use their electronic identification across national borders in any member country.

In practice, eID systems will provide a high degree of confidence that the individual has been sufficiently authenticated to greatly reduce the risk of identity theft and fraud. However, no system is foolproof. And eIDs also pose several challenges. For example, while some markets are experiencing widespread eID adoption, others are limited to in-person verification. Similarly, some markets are experiencing competing programs, and the idea behind identity documents is for them to meet globally accepted standards in order to allow international travel. As of yet, there's no globally accepted and interoperable form of eIDs. So while eIDs pose exciting opportunities for the future, they still need to overcome the hurdle of interoperability.

Alongside eIDs, the number of people using digital identity wallets is also increasing. Gartner predicts that half a billion smartphone users will regularly use digital identity wallets by 2026. The EU has also mandated the issuance of digital identity wallets by 2026 and has established a cybersecurity certification program for digital identity wallets. In the U.S., the Transportation Security Administration (TSA) is accepting digital driver licenses as proof of citizen identity at airports in many states. The rise of digital wallets could contribute to portable digital identity emerging as an alternative form of verification, which will create new opportunities, but also new fraud threats.



6. Increased use of behavioral biometrics to detect fraud

Bots are a significant tool for bad actors to automate and scale attacks like credential stuffing and fraudulent account creation. As their namesake implies, bots employ robotic patterns to increase the speed and consistency of attacks, which is both their biggest strength and largest weakness. Bots can do the work of millions, possibly billions, of humans in real time; however, to do this their behavior looks decidedly less human and more mechanical. Behavioral biometrics leverage AI and machine learning to detect bots by looking for non-human like behaviors in terms of mouse movement, keystroke velocity, touch screen interaction, and more. So as AI-powered bots continue to increase in sophistication, so will the use and sophistication of behavioral biometrics.

7. ICAO 2025 biometric passport will set new global gold standard for biometric system fairness and security

While it'll be several years before the highly anticipated ICAO 2025 biometric passport reaches mass adoption around the world, its still-evolving specifications provide critical insight into best practices for biometric systems across sectors. Based largely on ISO and IEC biometric standards, the new ICAO passport standard will provide best practices for biometric system fairness, biometric presentation attack detection, standard fingerprint and facial image quality, and more. This real-world use case of ISO and IEC biometric standards will guide the development and application of biometric systems across sectors for years to come.

Fraud Prevention Best Practices

How To Fight Fraud at Onboarding and Beyond

Really know your customer

Fraud manifests differently at each stage of the customer journey, but onboarding is an organization's first line of defense. Think of it this way: If your business services were a house, you'd want to stop that fraudster getting in when they first knock at the door. Because once they're inside, that's when they cause the most damage. Stopping fraud at onboarding increases security further down the line.

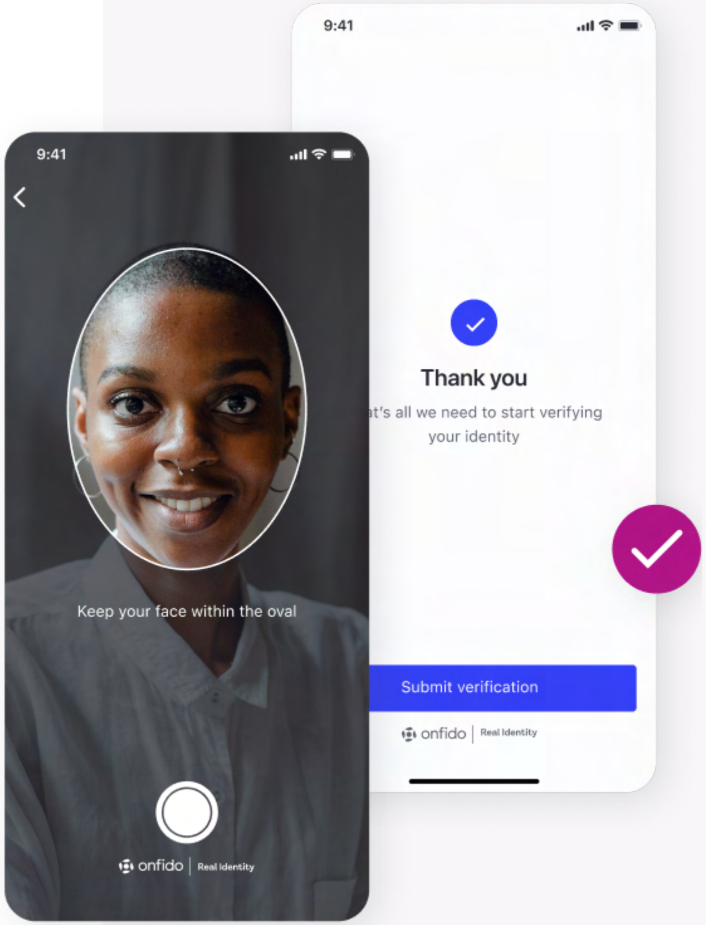
Stopping fraud starts by knowing your customer. For regulated industries such as financial services, identity verification as part of Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations is non-negotiable. For non- or less-regulated businesses, identity verification can also offer several benefits: fraud prevention being one of them.

Consider the integration aspect: SDKs versus APIs

How businesses integrate identity verification into their onboarding flows plays an important role in how protected they are from fraud. Leveraging out-of-the-box capture technology (such as an SDK) offers easier and more flexible integration, more consistent image quality, accessible UX, and better fraud deterrence.

Our SDK offers better protection against things like deepfakes because live capture greatly reduces the chance of digitally tampered image submission, and it can highlight injection attacks at the source.

Fraud is also constantly evolving, and opting for SDKs over APIs offers better protection against these evolving attack vectors, as the technology is designed to keep pace with changing fraud threats.



Keep your face within the oval

Thank you

t's all we need to start verifying your identity

Check for fraud throughout the customer lifecycle

While onboarding is an organization's first line of defense, fraudsters don't give up after day one. To protect customers from things like account takeover (ATO) and fraudulent transactions, businesses should build fraud prevention into the entire customer lifecycle.

A document and biometric check at onboarding helps to build trust in a customer's identity. We do this by matching the photo on an identity document to facial biometrics.

Beyond day one and during moments of high risk, businesses should employ biometric authentication to reconfirm a user is who they say they said they were at onboarding by comparing the new facial biometric with the document originally attached to the account.

To add an extra layer of security, businesses can adopt more control over how they store and manage users' biometric data. With bio-to-bio authentication, businesses can choose to store biometric data either on a device or on their own servers, giving them more flexibility across risk mitigation, data deletion policies, and privacy controls.

Adopt a "Zero Trust" strategy and implement cybersecurity best practices

Cybersecurity is key to ensuring a company's sensitive data is not compromised. Cybersecurity measures can prevent attacks such as unauthorized account access or phishing. AI is a powerful tool to help fight identity fraud and becomes even more powerful when leveraged as part of a larger Zero Trust strategy. Zero Trust as a security framework requires all users to be verified, authorized, and continuously validated when being granted access to networks or services. This helps businesses build more secure, connected identity experiences from day one, to day two and beyond.

A Zero Trust approach combines strong identity and access management (IAM) controls for employees and consumers that mandate identity verification alongside phishing-resistant multi-factor authentication (MFA), along with the use of public key infrastructure (PKI) to verify and encrypt communications. Digitally signing videos, images, and documents with PKI also helps verify the authenticity of digital media to help combat deepfakes at scale. These identity-centric solutions powered by AI will help defend against cyberattacks, minimize the insider threat, and quarantine compromised systems if an attack does occur.

Use AI to fight AI

There has been a lot of focus on the negative impacts of AI and the ways it helps bad actors commit fraud and scams. There is a general consensus that AI will play a part in increasing the volume and sophistication of fraud. However, AI also plays a crucial role in fraud prevention, too.

There are many different types of AI, and the tools leveraged by fraudsters (such as GenAI) are very different to those available to banks, financial institutions, and other businesses to combat threats.

Our fraud-prevention solution is built around AI that uses unique micro-model architecture combining over 10,000 machine learning models trained to detect specific fraud markers. With this type of approach, businesses can automate fraud prevention, detecting up to 50% more document fraud than approaches using generalized models.

Comprehensive Fraud Detection

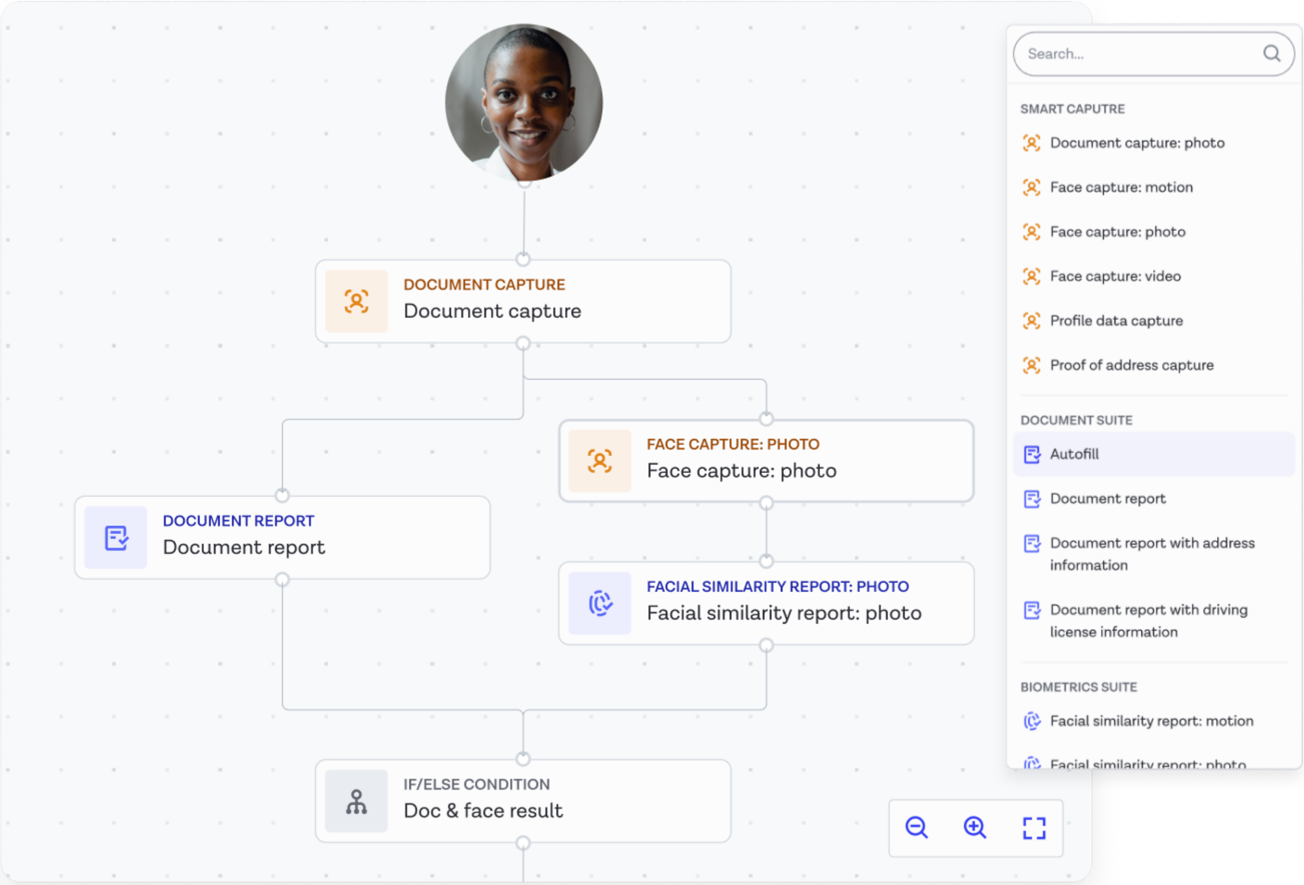
Respond and Adapt to Evolving Fraud With Flexible Workflows

Fraud is a constantly moving target. As the data in this report highlights, fraudsters continue to change their tactics – for example changing both the way they falsify documents, as well as which documents they falsify.

A comprehensive fraud solution should allow businesses to react to these evolving threats in real time. Shutting down threats quickly, before they impact an organization's bottom line. This approach also means businesses can dial fraud prevention measures up or down to balance the level of friction with the level of risk they feel comfortable taking on board, adapting that risk level for different scenarios.

Studio workflow builder

Studio allows businesses to configure a flexible blend of verifications and if-this-then-that conditions to build the ideal fraud prevention solution.



Adopt a Layered Approach to Fraud

A good fraud prevention solution won't rely on one prevention measure alone. There is no single silver bullet to fraud, because fraudsters are using multiple different techniques to attempt to bypass organizations' defense systems. This applies both at day one (onboarding) and beyond (at moments of high risk, or throughout the customer lifecycle).

Businesses need multiple layers of protection to weed out the fraudsters. This can include a combination of:

Document verification: Users take a photo of their identity document and AI verifies the visual, data, and metadata elements of the document in seconds to confirm whether it's genuine or fraudulent.

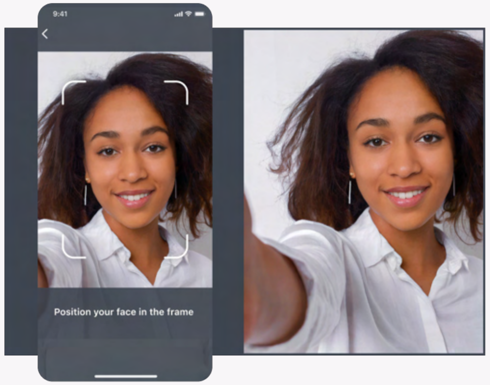
Biometric verification: A biometric step helps verify that an identity document belongs to the person presenting it, protecting businesses from stolen IDs and impersonation fraud. End-users simply capture their face and we compare the photo on the ID to their biometrics.

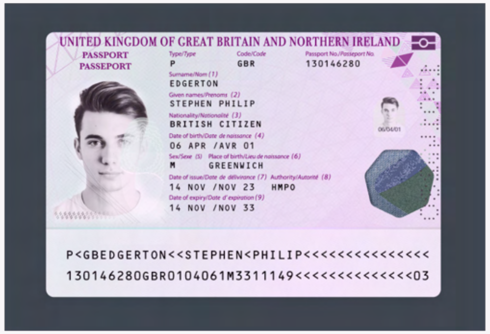
Repeat fraud detection: Fraudsters tend to re-use information (such as names, document numbers, and faces) across different checks. We detect repeat information across documents and check for duplicate faces within an organization's system to catch repeat fraudsters.

Data verification: Trusted data sources, including global databases; watchlist, sanctions, and PEPs lists; and automated proof of address help build a more accurate picture of a user's identity.

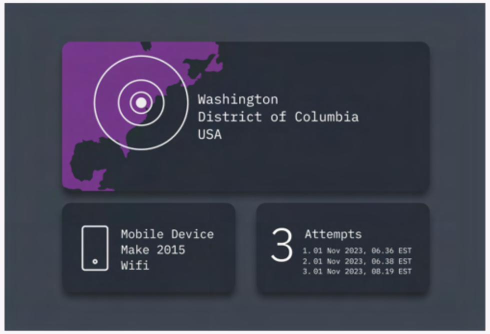
Passive signals: Device intelligence, geolocation, and repeat fraud signals work in the background alongside a document and biometric check to detect other fraud markers without impacting UX.

Combining a layered approach with a Zero Trust framework (which requires all users to be verified, authorized, and continuously validated when being granted access to networks or services) helps businesses build more secure, connected identity experiences from day one, to day two and beyond.




UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
PASSPORT
PASSEPORT
Type/Type P
Code/Code GBR
Passport No./Passeport No. 130146280
Surname/Nom (1) EDGERTON
Given names/Prenoms (2) STEPHEN PHILIP
Nationality/Nationalité (3) BRITISH CITIZEN
Date of birth/Date de naissance (4) 06 APR /AVR 01
Sex/Sexe (5) M
Place of birth/Lieu de naissance (6) GREENWICH
Date of issue/Date de délivrance (7) 14 NOV /NOV 23
Authority/Autorité (8) HMPO
Date of expiry/Date d' expiration (9) 14 NOV /NOV 33
06/04/01

P<GBEDGERTON<<STEPHEN<PHILIP<<<<<<<<<<<<<<<
130146280GBR0104061M3311149<<<<<<<<<<<<<<03


Washington
District of Columbia
USA

Mobile Device
Make 2015
Wifi

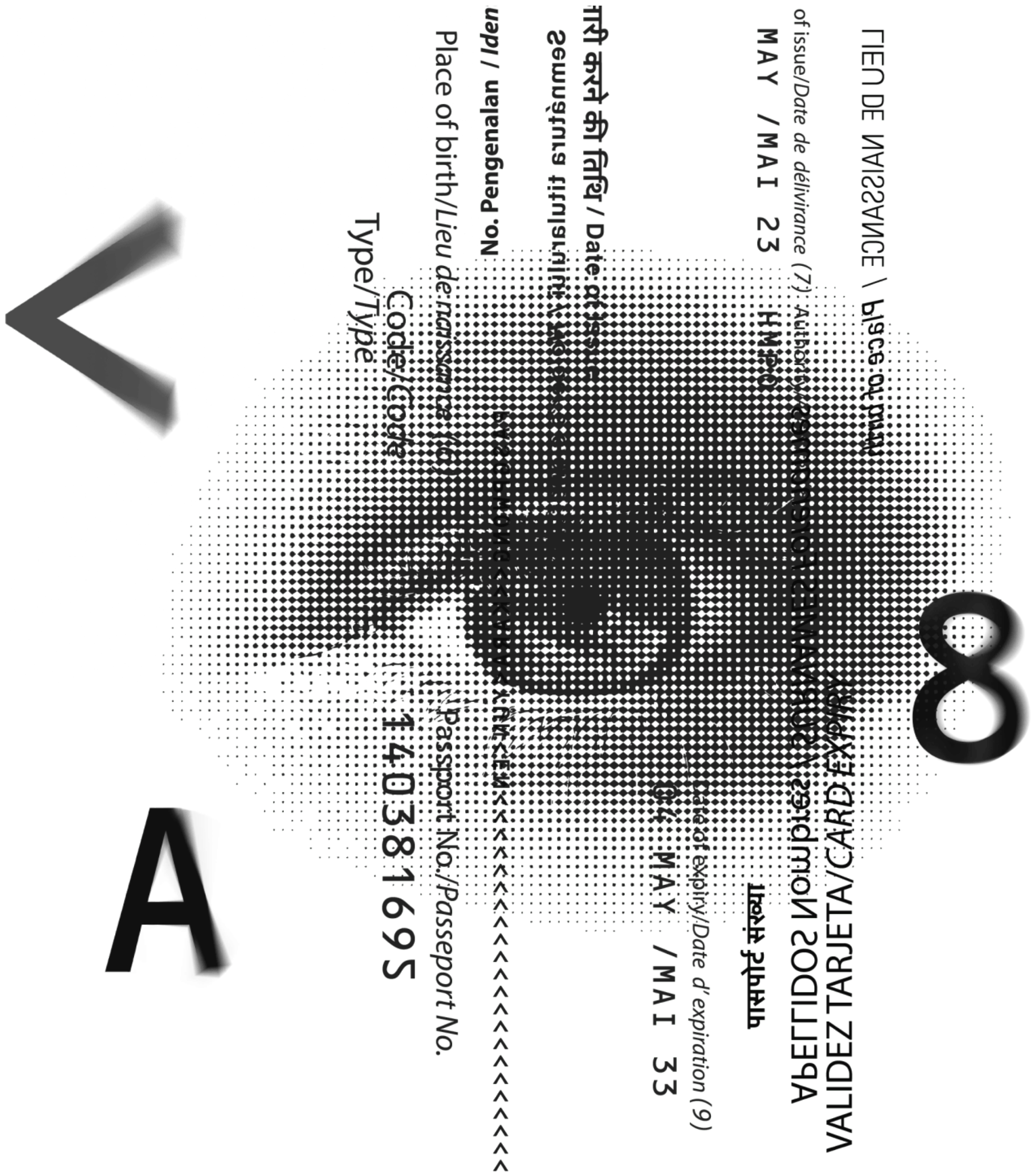
3 Attempts
1. 01 Nov 2023, 06.36 EST
2. 01 Nov 2023, 06.38 EST
3. 01 Nov 2023, 08.19 EST

Lean Into Pattern and Risk Analysis

Preempting and catching fraud relies on looking for patterns in the data. Any good fraud solution should detect such patterns, for example repeat fraud (with solutions like Repeat Attempts and Known Faces).

Fraud Lab

Our AI is also trained to specifically solve for the problem of identity fraud. Trained and tested by our in-house Fraud Lab, our unique micro-model architecture combines over 10,000 machine learning models designed to detect specific fraud markers. Our micro-models analyze pixel-level variations in document color, shape, and texture to accurately assess authenticity



Type/Type
Code/Code
Place of birth/Lieu de naissance
Passport No./Passeport No.
No. Pengenalan / Iden
MAY / MAI 23
04 MAY / MAI 33
Date of expiry/Date d'expiration (9)
APELLIDOS Nombres
VALIDEZ TARJETA/CARD EXPIRY
A
8

About Entrust

Entrust is an innovative leader in identity-centric security solutions, providing an integrated platform of scalable, AI-enabled security offerings. We enable organizations to safeguard their operations, evolve without compromise, and protect their interactions in an interconnected world – so they can transform their businesses with confidence. Entrust supports customers in 150+ countries and works with a global partner network. We are trusted by the world's most trusted organizations.

About Onfido

Onfido, an Entrust company, makes digital identity simple. The platform allows businesses to tailor verification methods to individual user and market needs in a no-code, orchestration layer – combining the right mix of document and biometric verifications, trusted data sources, and passive fraud signals to meet their risk, friction, and regulatory requirements. Partnering with over 1,200 businesses globally, Onfido helps millions of people access services every day – from billion-dollar institutions to hyper-growth start-ups.

entrust.com | Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION