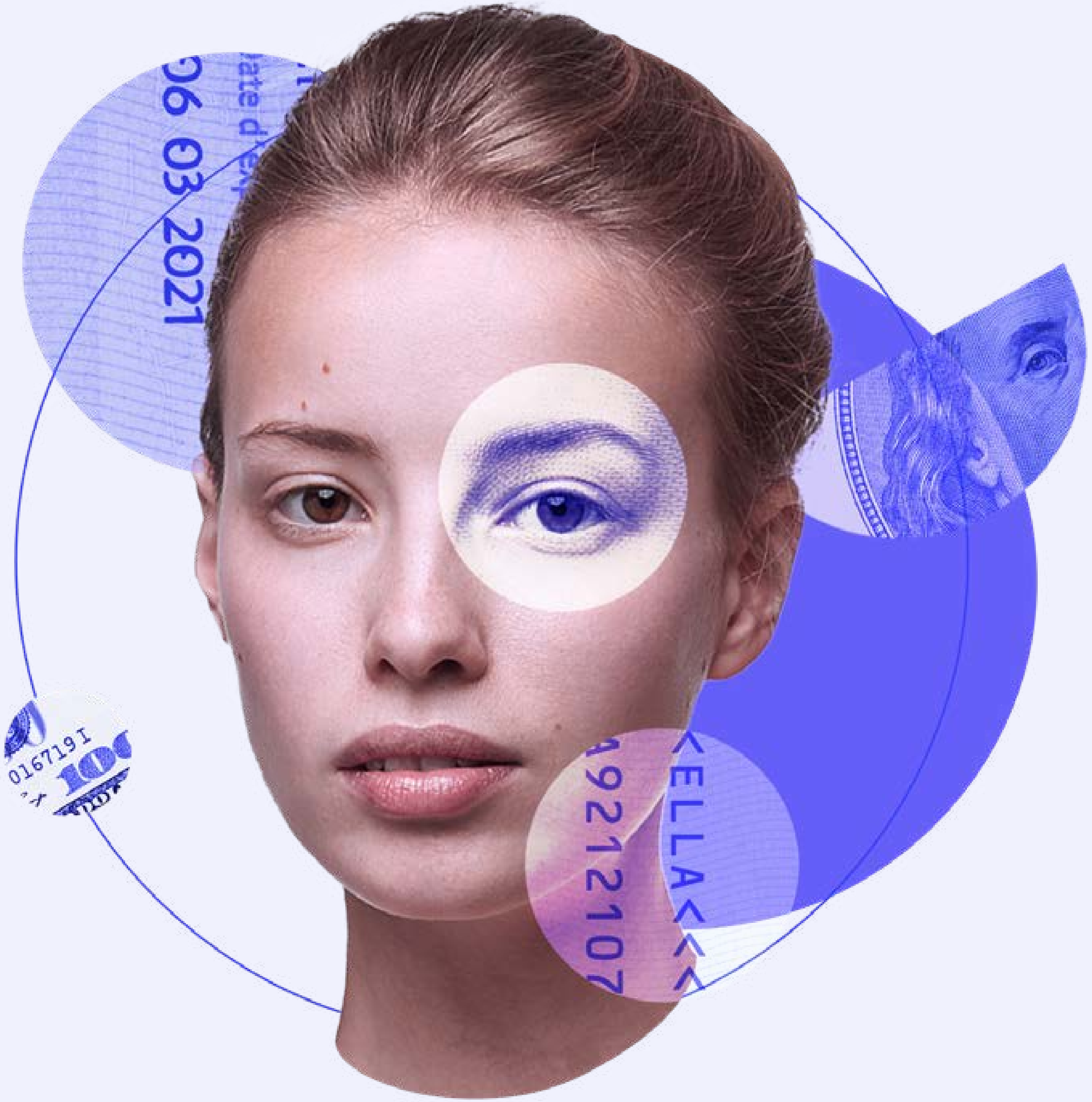
Onfido's Identity Fraud Report 2020

The developing trends and techniques businesses need to know about – and protect against – in the year ahead.

onfido



Contents

3 Foreword

4 Key takeaways from 2020

8 Methodology

9 Trends

Data stories

10 ID fraud is increasing

11 Covid-19 is driving the rise in ID fraud

12 Financial and Professional Services have been the hardest hit

13 Fraudsters are choosing both quality and quantity

15 ID fraud is no longer just a 9-5 job

16 **Deep dive** Why Covid-19 is driving the rise in ID fraud

10 Techniques

Data stories

22 National ID Cards are the most frequently defrauded documents

23 Counterfeiting is the most popular method of ID attack

25 Most fraudsters miss the detail on data

26 Biometric fraud is a developing landscape

29 **Deep dive** Four emerging trends in biometric fraud

33 Tips

34 What to watch out for in 2021

38 **Best practice** How to strengthen your ID fraud defenses

INTERPOL

Foreword

By Interpol

“Identity document (ID) fraud can take different forms, and both false and genuine documents are used to perpetrate a variety of frauds.

The fraudulent use of identity and travel documents therefore presents a threat to the security of countries and their citizens, the economy, and global commerce, and is often linked to organized crime, money laundering and terrorism.

Document verification and authentication are crucial in ensuring that the documents presented are both genuine and in the possession of the rightful holder.

Increasingly, identity documents are required to be verified in the form of a two-dimensional scan or image – a task previously considered either impossible or very difficult. Identity and travel documents were traditionally designed to be verified by trained personnel using a variety of tools, but that task is increasingly being taken over by artificial intelligence.

Through this publication, Onfido’s team of experts provides a useful reference guide for practitioners on fast-growing forms of identity document fraud and reflects on the continuous evolution of ID fraud. Onfido’s Fraud Index also addresses specific topics and includes real-life statistics based on their work to uncover deception before it leads to criminal activity.”

> “
> Document verification and authentication are crucial in ensuring that the documents presented are both **genuine** and in the possession of the **rightful holder.**

Key takeaways from 2020

In 2019, data from Onfido's global clients showed that identity fraud is sophisticated and serious. Professional fraudsters work 9-5, employing a range of creative and complex techniques to increase efficiencies and maximize profits.

This year, all our lives have been disrupted by Covid-19. The fraud landscape has been impacted, too – and not for the better.

Identity document fraud is on the rise

Fraud of all kinds has increased during the pandemic. Experian reported a 33% increase in fraud[1] in the first month of the UK lockdown alone, while citizens in the US are estimated to have lost $145 million[2] so far this year. ID fraud is no different.

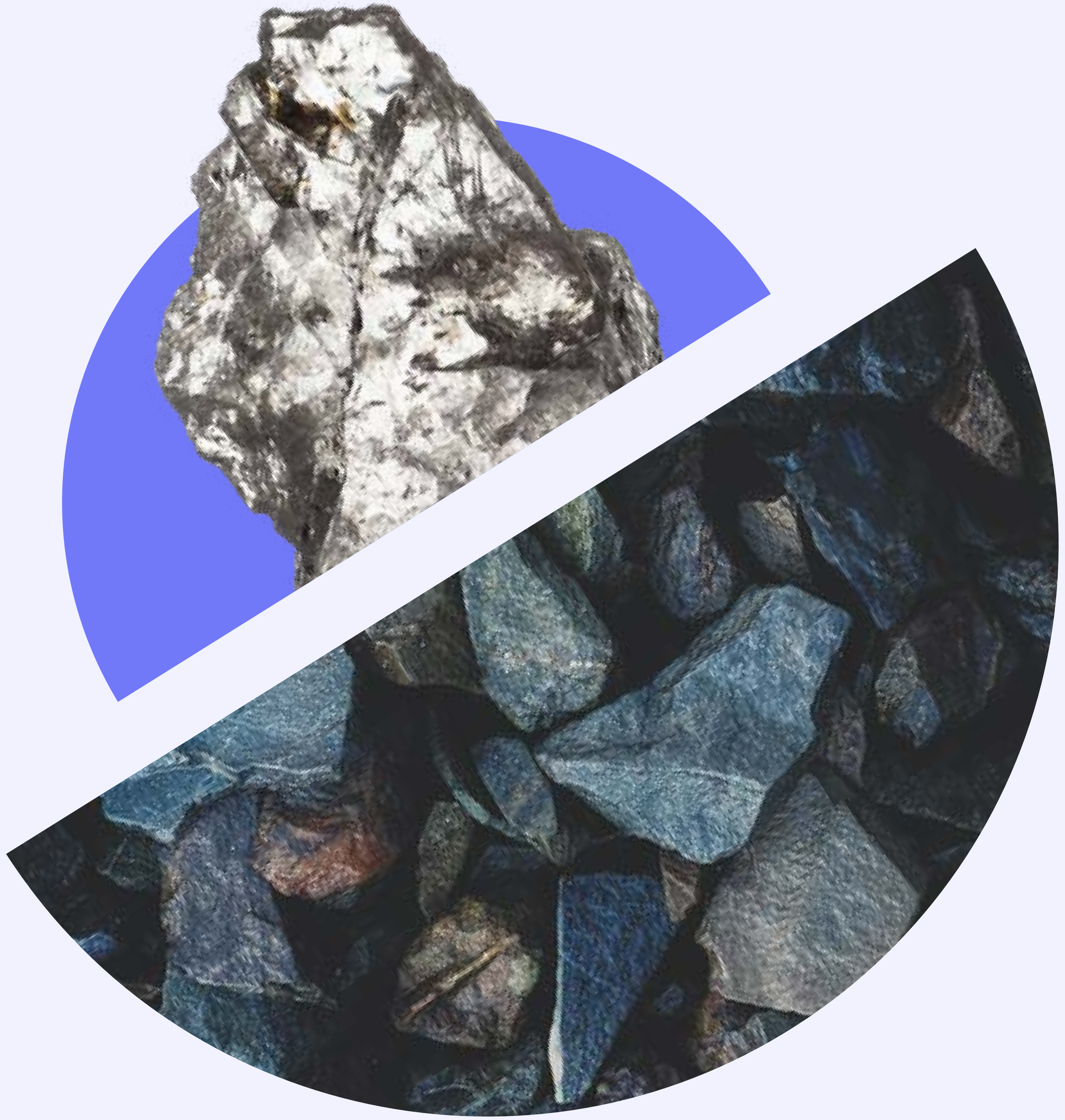
Our data shows that global fraud rates have risen from where they were in 2019. In a turbulent economy there's more opportunity for fraud – and more people are taking advantage of that fact. The 9-5 pattern we identified last year has changed: fraudsters are no longer taking the weekends off. Attacks are now happening constantly, and aren't likely to slow down as the post-Covid landscape continues to shift.

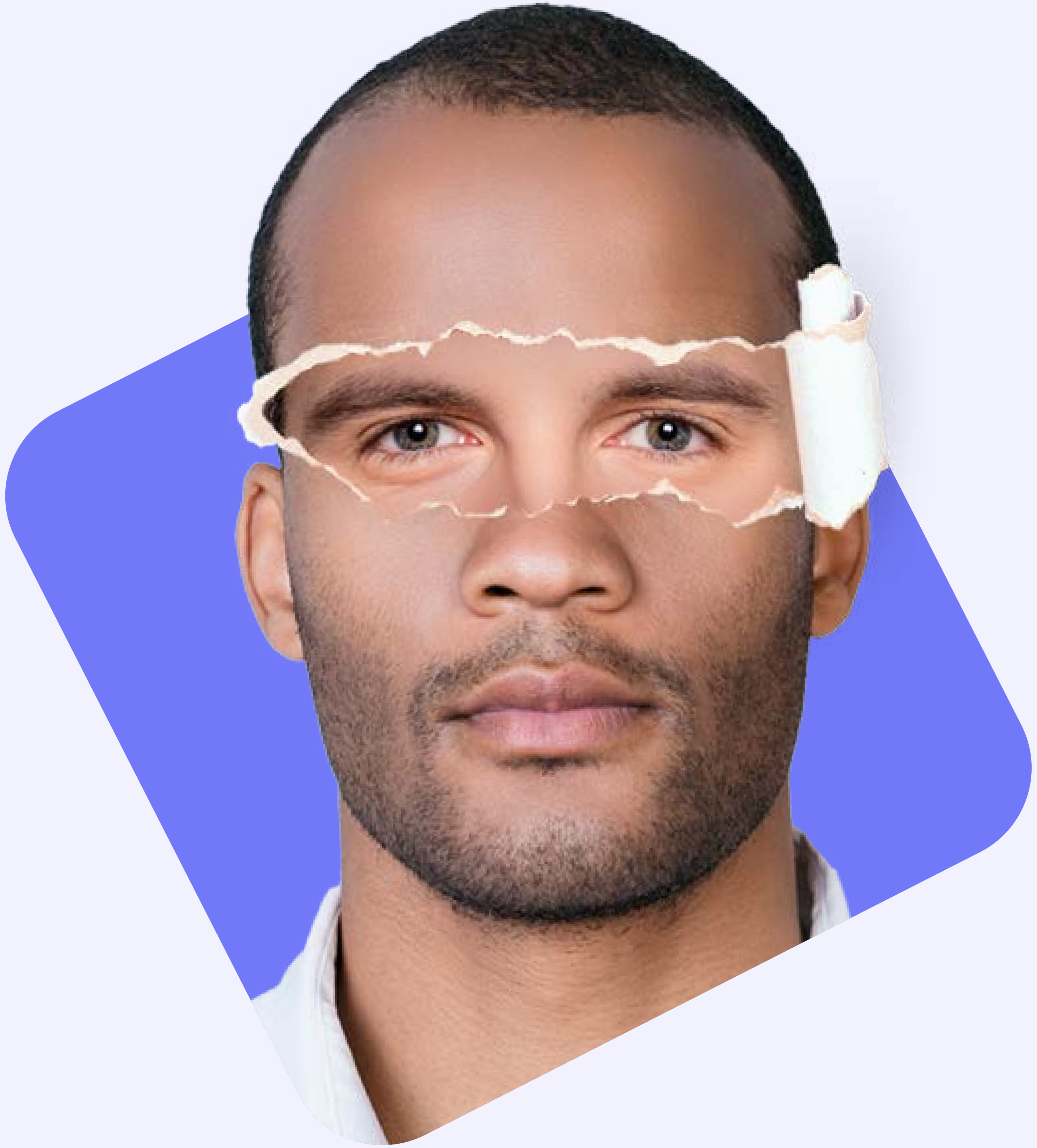
1. Source: www.experianplc.com/media/news/2020/fraud-rate-rises-33-during-covid-19-lockdown/
2. Source: nytimes.com/2020/09/23/us/coronavirus-scams-ftc-reports.html

Fraudsters are choosing both quality and quantity

Professional fraudsters have been busy, adapting their methods to make the most in the surge of online activity. But now others are getting in on the game, too.

This year, we identified an uptick in 'unsophisticated' fraud. Unfortunately, this doesn't mean it's easier to catch. Instead, businesses now need to fight the battle against ID fraud on two fronts. Systems need to be able to handle **sophisticated attacks** from criminal gangs, as well as **high volumes of attacks** from non-professional fraudsters.





Biometric fraud is a fast developing space

While the majority of biometric fraud remains rudimentary, it’s a fast developing risk landscape. For the first time, we saw Deep Fakes being used to attack our video product.

Replay attacks are also on the rise, as an easier alternative to single-use 2D and 3D masks. Meanwhile, coercion poses a future threat that businesses and technology providers will have to think carefully about how to tackle.

Methodology

At Onfido, our team of fraud specialists verifies millions of identities every year. We are experts in remote identity verification, helping over 1,500 clients detect fraud across 4,600 document types from 195 countries.

This Identity Fraud Report shares the insights we've gained on the state of remote identity fraud over the past year. The following infographics illustrate some of the key developing trends we've observed, drawn from our data*.

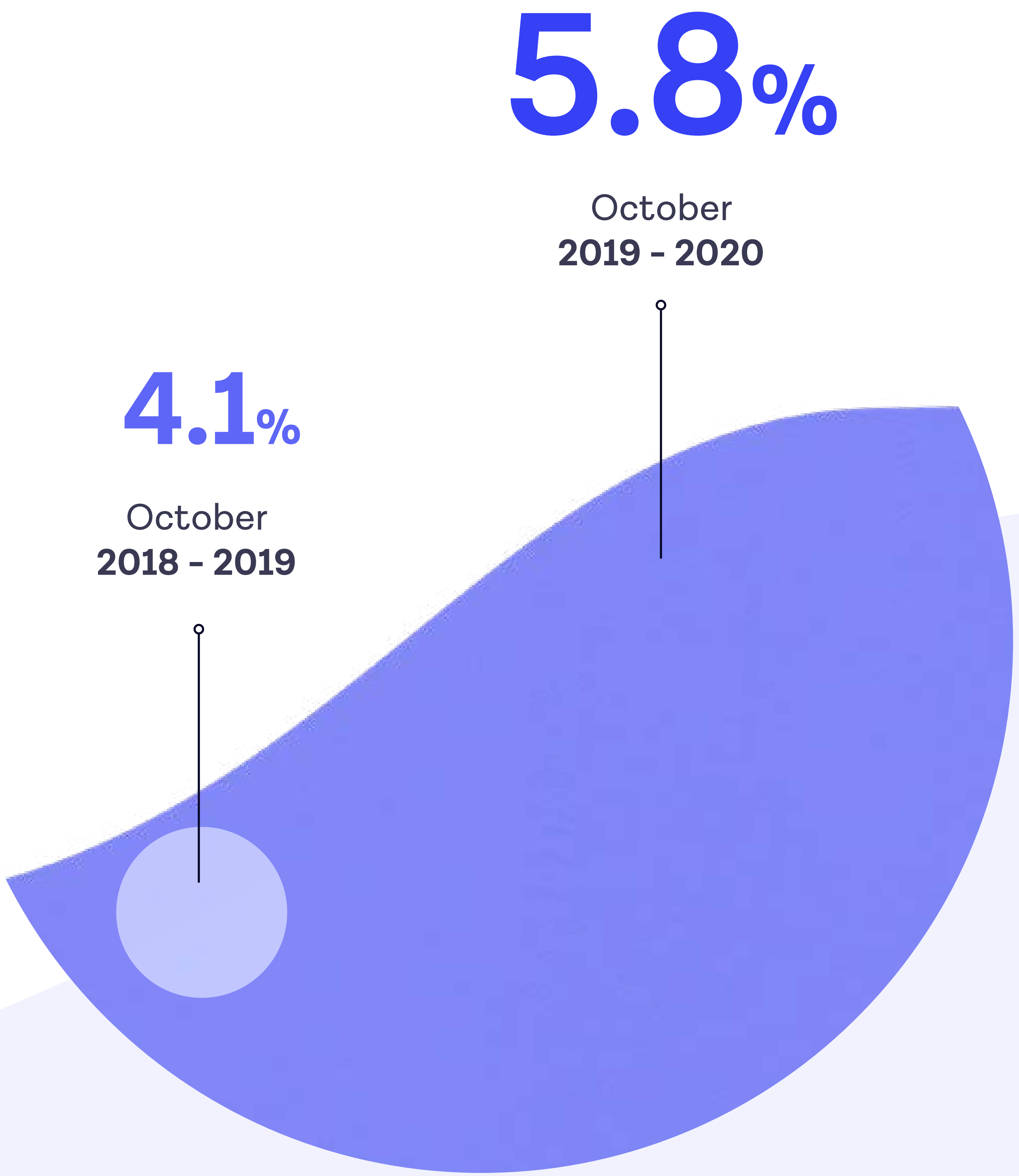
*The data for this study was collected from October 2019 - October 2020 and normalized by client and industry distribution.

Trends

ID fraud is increasing

Our data bears out what many of our customers have felt anecdotally: that risk of identity fraud is increasing, and attacks are happening more frequently.

In the year from October 2018 - 2019, we saw an average ID fraud rate of 4.1%. Over the last year, that's jumped up to 5.8% – and that trajectory looks set to keep trending upwards. There are a number of reasons for this, the key ones being the ubiquity of stolen data and the Covid-19 pandemic opening up more opportunities for fraud.

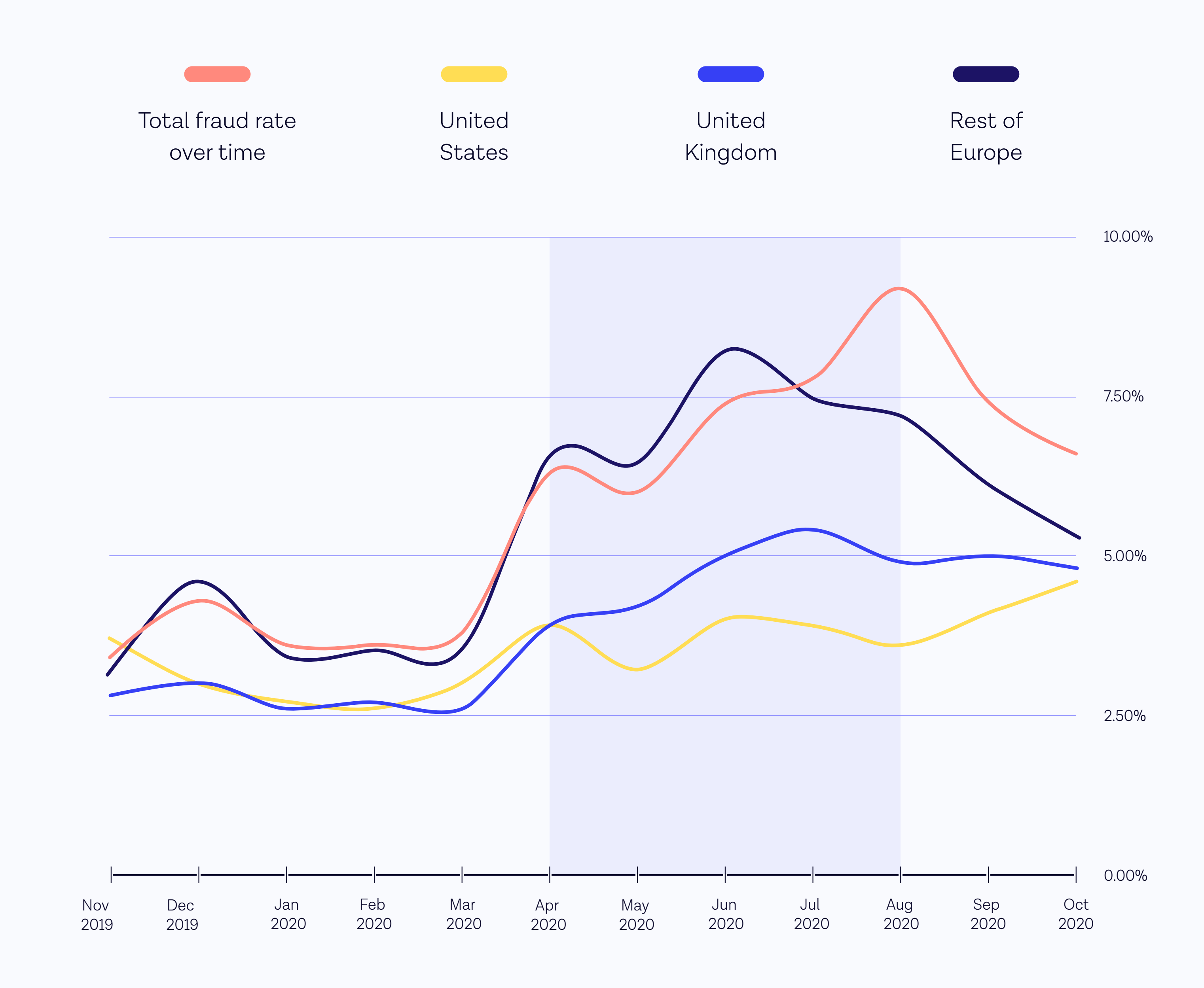


Covid-19 is driving the rise in ID fraud

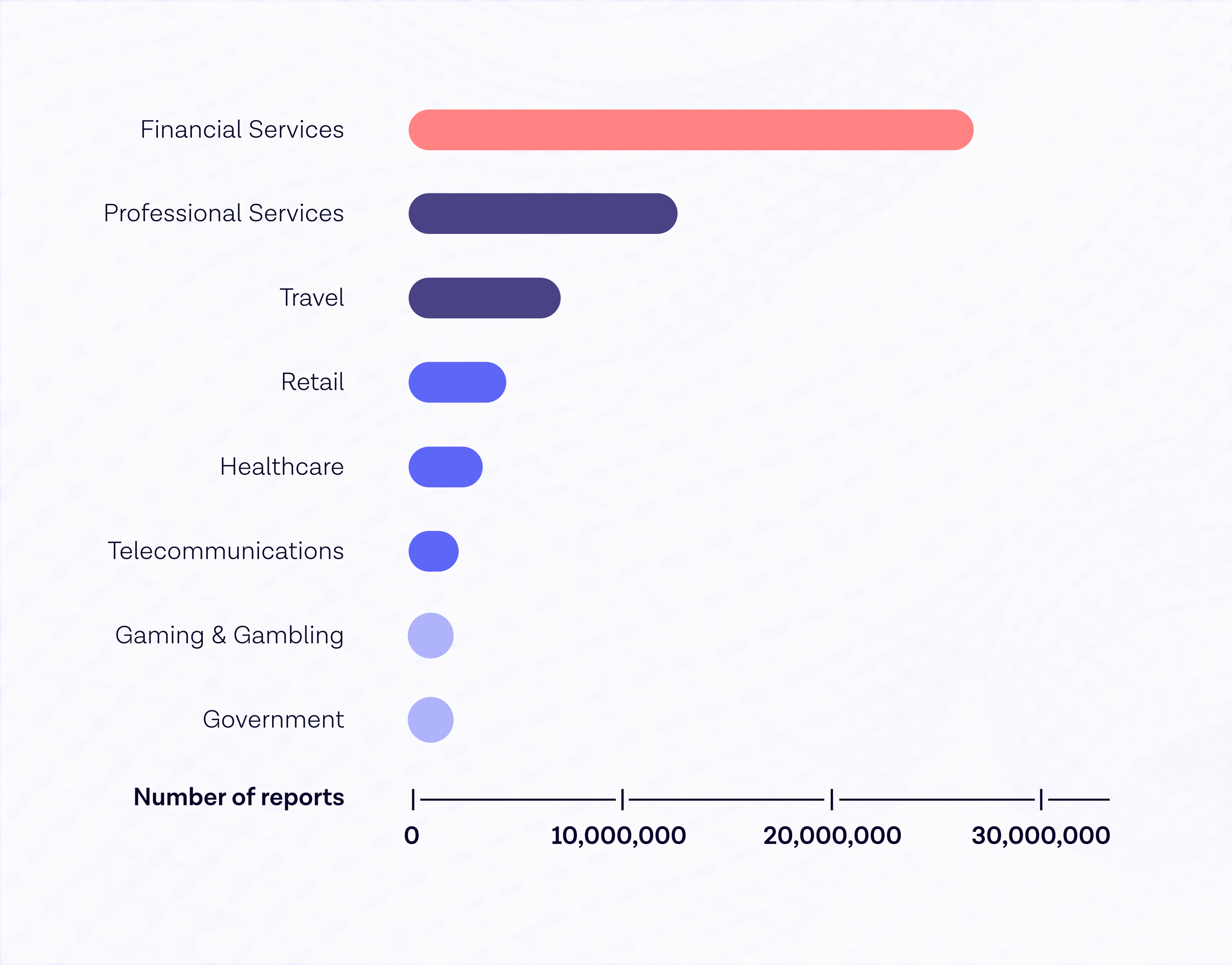
Unsurprisingly, Covid-19 has had a significant part to play in the uptick in attempted ID fraud. Our data shows that fraud rates held steady for the first few months of the year, then rose sharply from April 2020 onwards.

It's no coincidence that this was when most of the world was entering the first phase of lockdown: more people at home and more businesses transitioning online made fertile ground for identity fraud. Fraudulent activity peaked in July and August, and has started to decline slightly since. But as large parts of Europe encounter a 'second wave' and re-enter lockdown, it's likely fraud rates will start to climb again in the last few months of the year.

Covid-19 is driving the rise in ID fraud



Suspected fraud rate by verticals



Financial and Professional Services have been the hardest hit

Financial Services have been most impacted by identity fraud this year, followed closely by Professional Services.

The correlation isn't surprising; industries that fall under Professional Services, like Legal and Investment, are in close proximity to the financial ecosystem. When fraud increases for one, we can expect to see it rise for the other. Financial services are always at high risk of identity fraud, but suspicious behavior is harder to spot now – spending habits have changed dramatically, even among legitimate users. With so much volatility in the market, businesses across all industries need to be extra-vigilant.

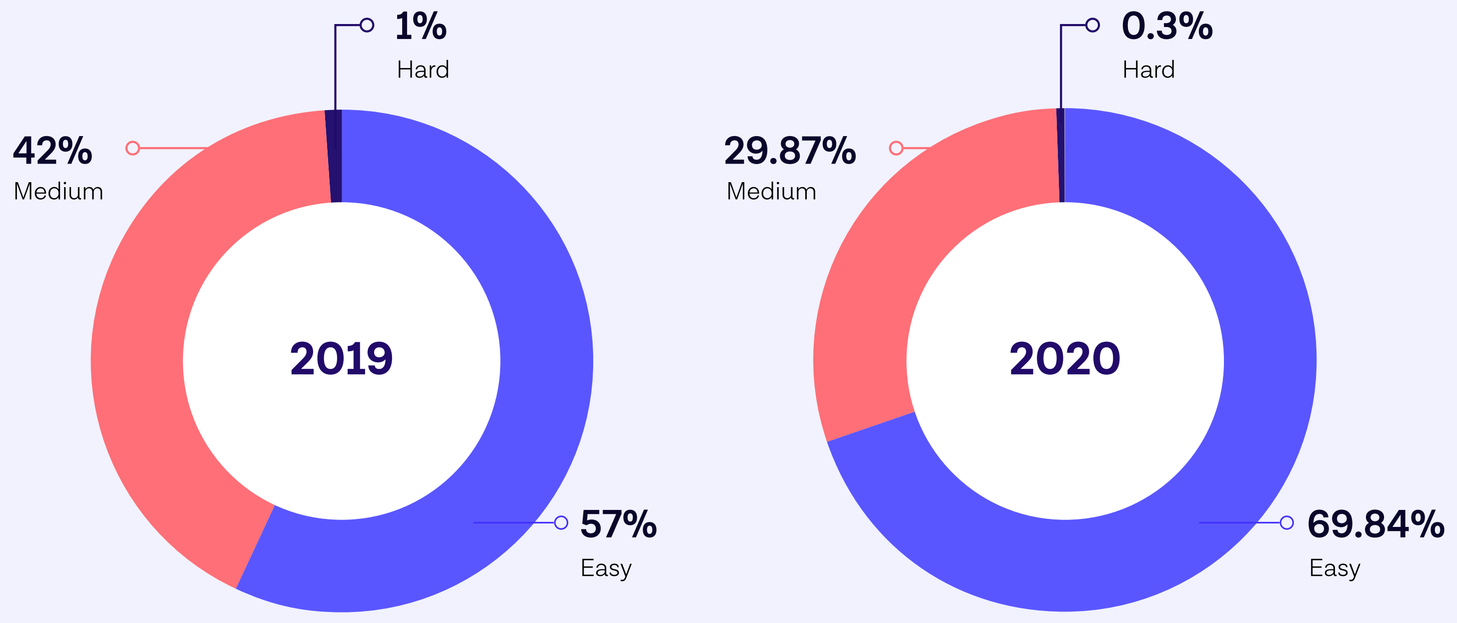
Fraudsters are choosing both quality and quantity

This year, the proportion of 'easy' fraud has grown from 57% in 2019's Fraud Report,[3] to almost 70%. But that doesn't mean that fraudsters are getting careless, or that businesses can afford to take their eye off the ball.

There are a few reasons that 'easy' ID fraud has increased. One is that we've slightly adjusted our own categories to match the rising levels of fraud sophistication in the market. What was once considered 'medium', like detecting the wrong printing color profile on a document, would now be categorized as easy. Essentially, hard fraud is getting harder. That's set the bar higher elsewhere, too. This adjustment means there's now a greater volume going into the 'easy' fraud bucket, and it's more sophisticated than before.

[3] Source: onfido.com/resources/home/fraud-index-2019

Fraud sophistication

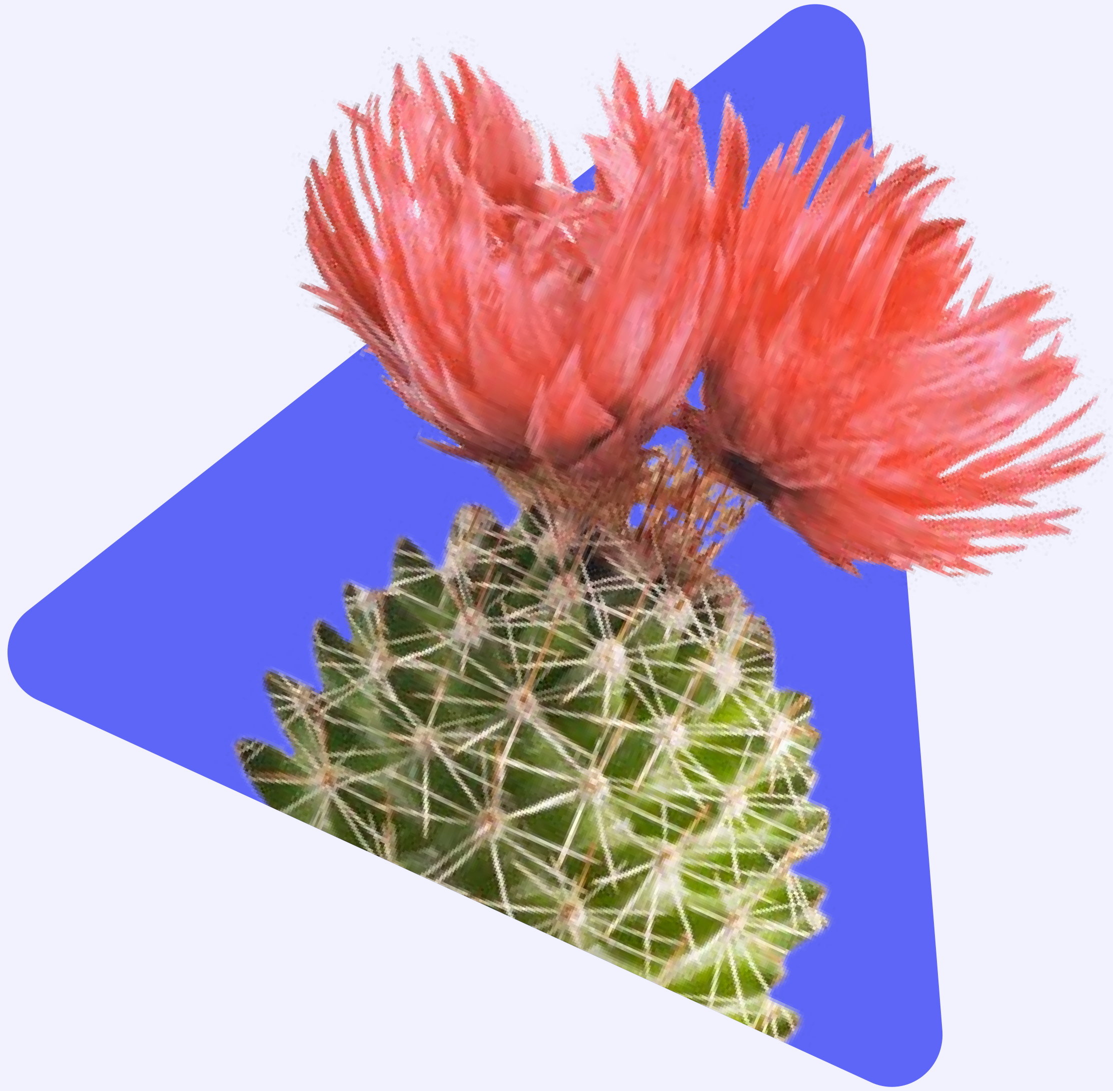


Easy
Where document elements are clearly wrong—for example an obviously wrong font, or where the photo has been clearly attacked.

Medium
Less obvious errors, such as using fonts that are less visibly incorrect, a photo printed using the wrong technique, or imitated security features.

Hard
Cases which would only be detectable with enhanced knowledge of document manufacturing, security features, printing, and deliberate mistakes.

Hard fraud is getting harder



But there's another reason why 'easy' attacks have increased and again, it's down to Covid-19.

As we've seen, there's been a higher volume of ID fraud attacks overall, but the amount of 'hard' attacks has stayed the same, at under 1%. This tells us more attacks are happening at the 'easy' end of the spectrum, suggesting that non-professional fraudsters are getting in on the game.

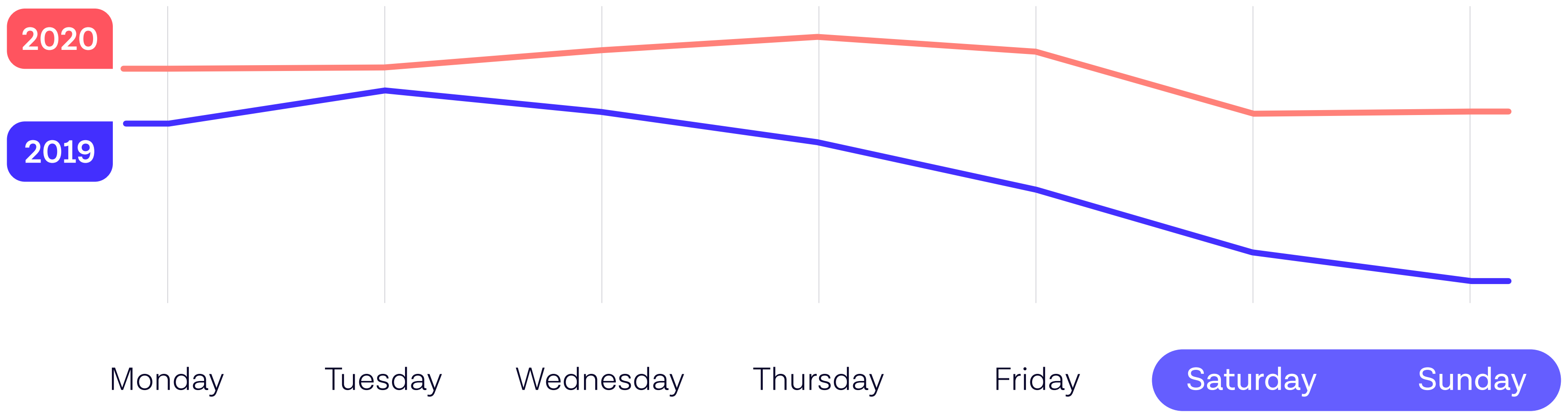
The disruption caused by the pandemic means that there's both more opportunity for first-time fraudsters, and more financial need. That's bad news for businesses. Now, not only do they need to keep on top of complex, high-impact attacks by professional fraudsters, they also need to manage higher volumes of attacks from everyone else. Both quality and quantity need to be considered when it comes to effectively fighting ID fraud.

ID Fraud is no longer just a 9-5 job

In 2019, our Fraud Report[4] showed that ID fraud was a 9-5 job: attacks were higher on weekdays, but dropped off over the weekends.

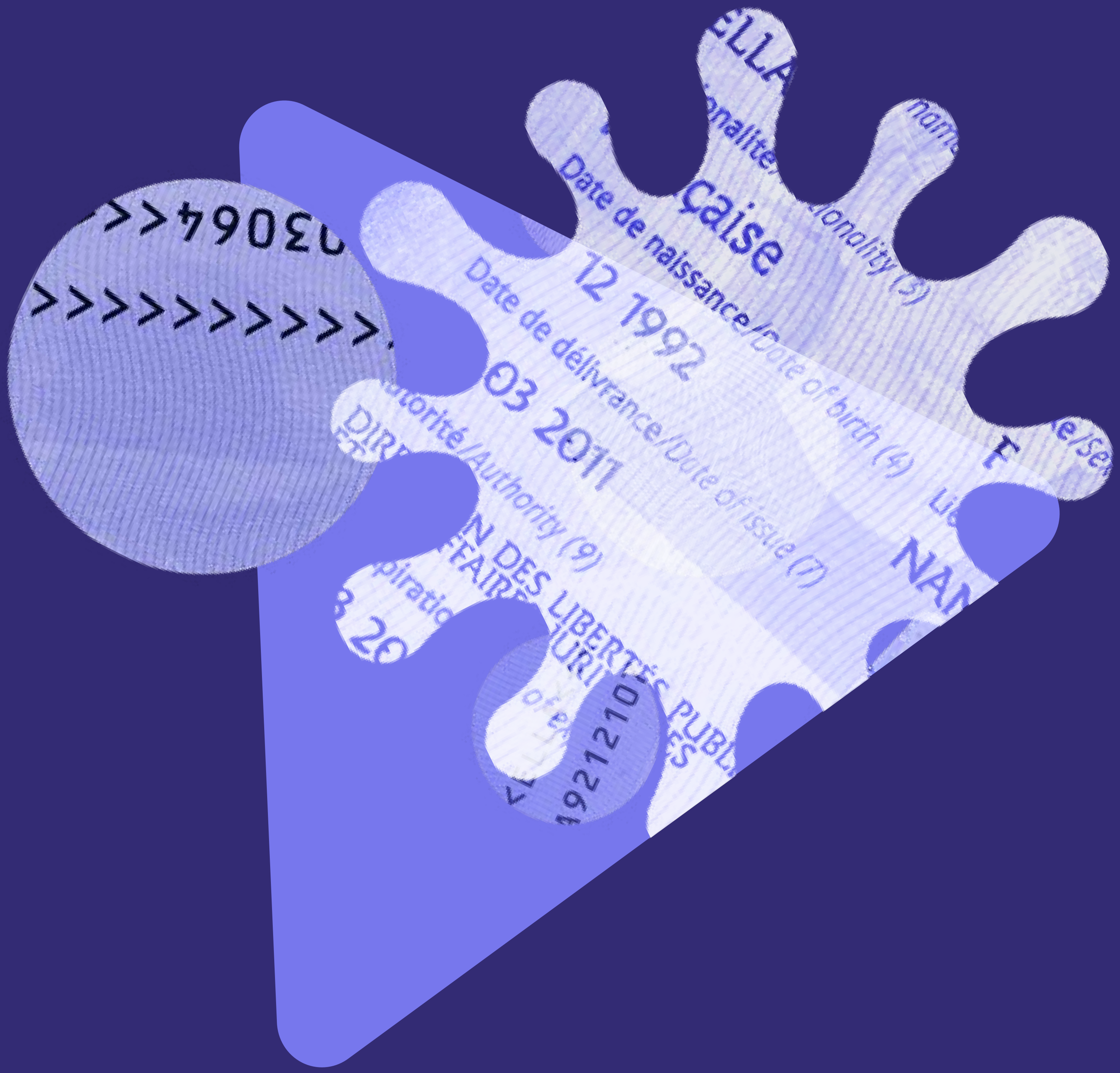
This year, that's changed. Now, the suspected fraud rate is staying almost level over all seven days of the week. Once again, we can attribute this to the pandemic. Fraudsters are at home more, and they're essentially working 'overtime' – just like everyone else. And now they're being joined by the ranks of first time or 'unprofessional' fraudsters, too. In short, there are more fraudsters in the 'talent pool', and they're working tirelessly to get the greatest possible returns. Fraudsters aren't taking a break and that means businesses can't afford to, either. Anti-fraud protections need to work against high volumes of unsophisticated attacks as well as more complex fraud from professionals - and they need to work around the clock.

Fraud day of the week seasonality



[4] Source: onfido.com/resources/home/fraud-index-2019

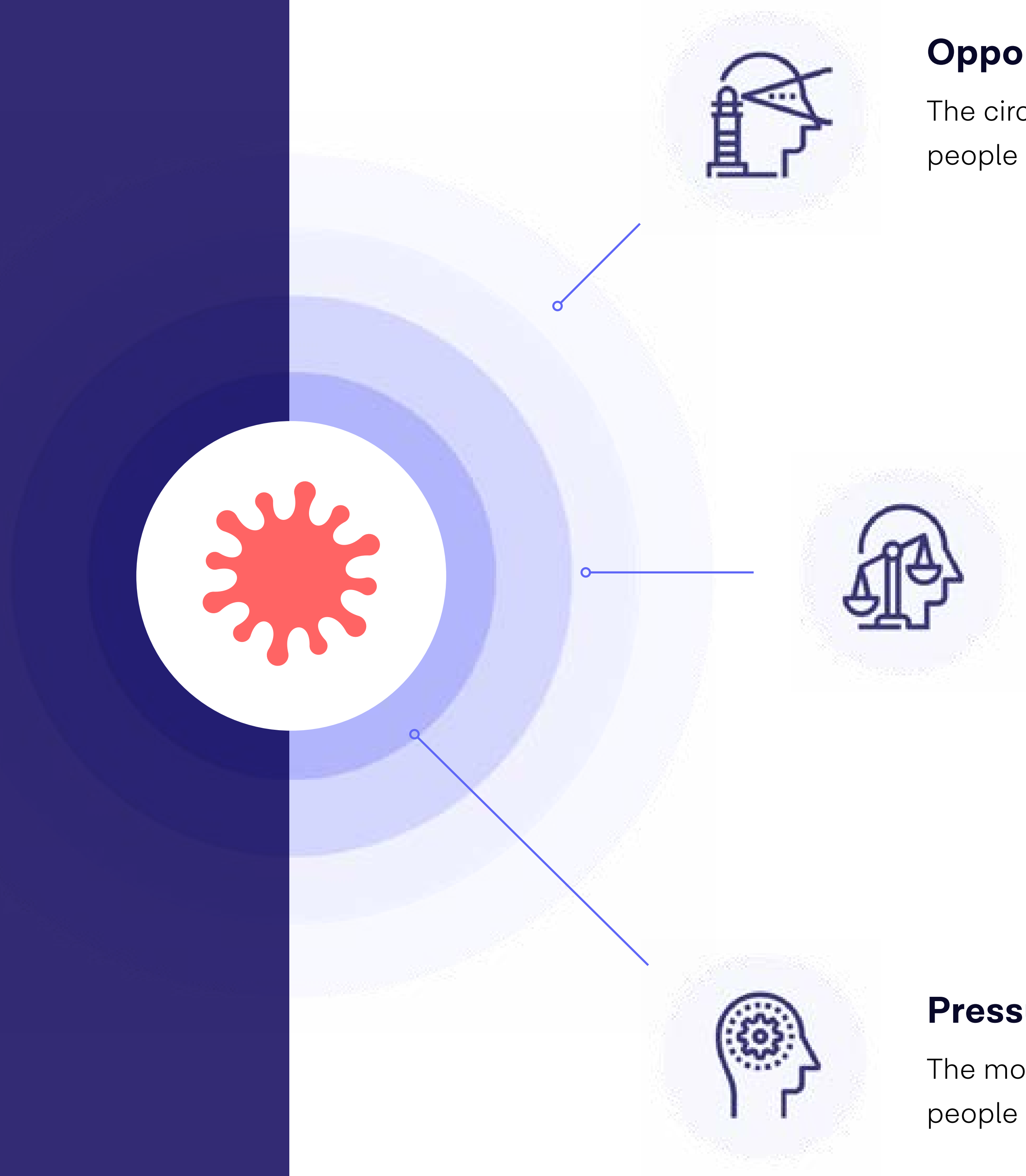
Deep dive



It’s been widely reported that fraud has increased during Covid-19

But what exactly is driving the change?

The pandemic has created a perfect storm for fraud. In any crisis, fraud rates tend to increase. That’s because fraud’s usually a product of three factors: opportunity, rationalization and pressure. Thanks to Covid-19, all three of these factors have intensified.



Opportunity

The circumstances that allow people to commit fraud

Rationalization

The frame of mind that allows people to justify their dishonest actions.

Pressure

The motive or incentive for people to commit fraud

Opportunity has opened up because so many businesses are moving online

As we know, detecting any fraud – and ID fraud in particular – becomes exponentially harder in a digital environment.

When documents and even faces are presented in 2D, it's much trickier to identify the tell-tale signs of manipulation that would be obvious in a 3D setting. On top of that, successful fraud is more scalable online. Once a fraudster finds a loophole, they can exploit it multiple times before moving on.

Take the example of opening a bank account – it simply wouldn't be possible to get away with more than a couple of attempts in person before getting caught. Online, it is. And now more goods and services are available digitally than ever before, so the potential payoff for fraudsters is even higher.

Rationalization has become easier for fraudsters, too

Admittedly, it’s been a hard time for most businesses, so some might feel bad about taking advantage. But on the other hand, a lot of businesses have received bailouts and stimulus packages. This might contribute to a general feeling that ID fraud is a victimless crime. If costs fall onto faceless corporations rather than individual people, and those corporations are being government-funded anyway, fraudsters might rationalize that no real harm’s being done.

This is especially true of the increasing number of first time and ‘unprofessional’ fraudsters we’ve seen this year. For those people, it’s likely that fraudulent behavior is being driven by genuine financial pressure. Many have experienced job losses, and feelings of financial wellbeing have suffered significantly.[5] It’s forced some into a corner. Millions of unbanked adults across the world rely on cash; now, they can’t use it. The trend towards digital and contactless payments has disenfranchised some of society’s most vulnerable, leaving them little option but to turn to ID fraud to open bank accounts.

[5] Source: www2.deloitte.com/uk/en/pages/press-releases/articles/customer-financial-wellbeing-deteriorates-while-trust-in-banks-rises.html

Whether professional or unprofessional, this confluence of factors has meant that more ID fraud is happening than ever before

Fraudsters have had to get creative to adapt to the 'new normal'. We've seen some interesting techniques and behaviors emerging thanks to Covid-19, especially when it comes to money mules.

Typically, professional fraudsters will approach people on the street to become money mules. They give them money and ask them to open an account in their own name, before transferring the money to another account to launder it. Now, they can't do that in person – and it's left them with a backlog of money to launder. To fill the shortfall, professional fraudsters have been preying on the recently unemployed via online job boards.[6] Many have been unwittingly recruited via listings for 'financial transfer analysts' and similar, and it's actually making life easier for fraudsters. It enables them to create scores of digital accounts across neobanks, remittance, and payments platforms to launder money at scale.

[6] Source: https://www.thetimes.co.uk/article/criminals-con-the-unemployed-into-becoming-money-mules-nhhsc302v

Techniques

National ID Cards are the most frequently defrauded documents

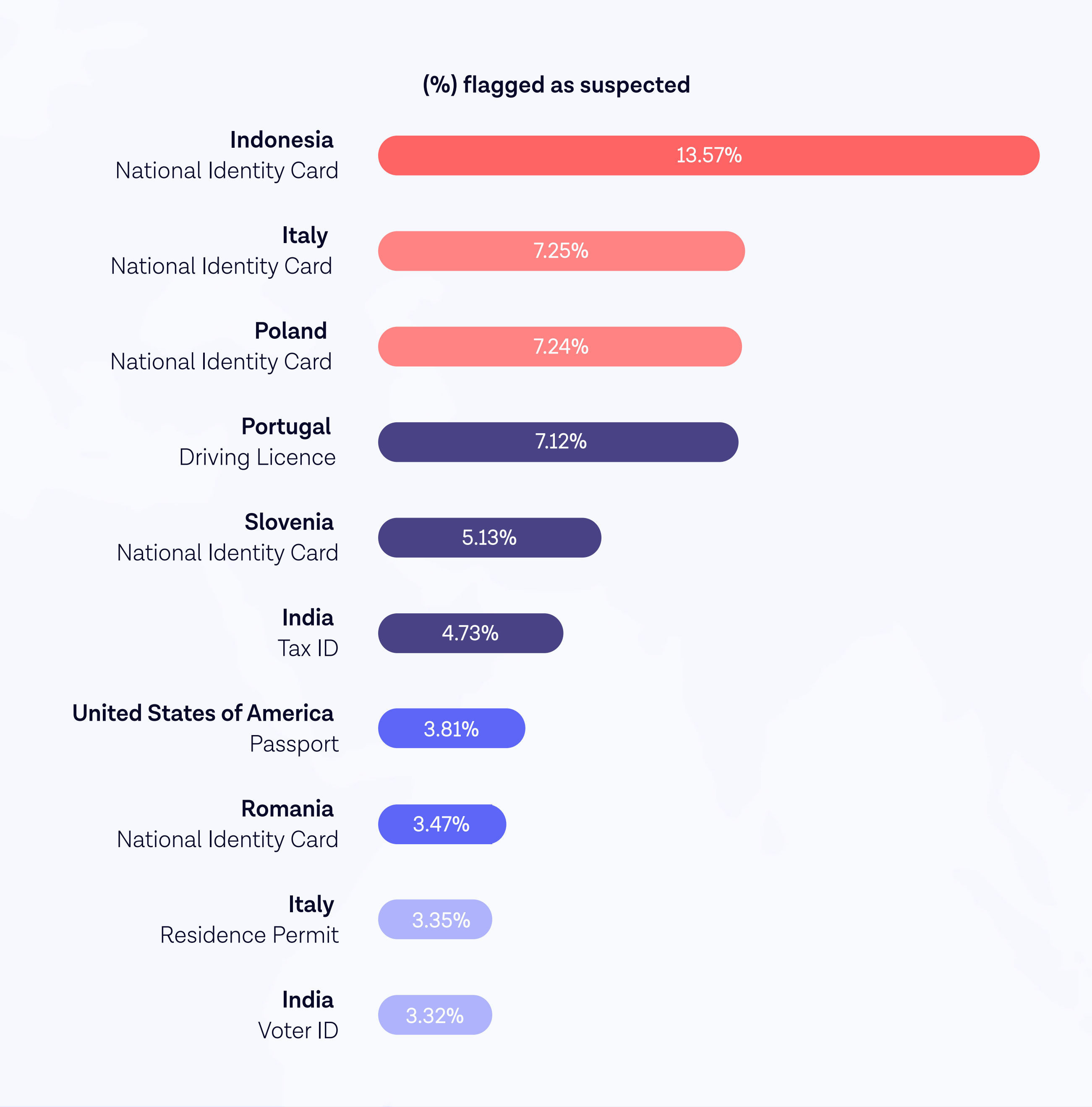
The fraud rates our clients see will largely depend on where they and their customers are based; it's no surprise the businesses in the US see a higher volume of US documents, and those in Europe see more European documents.

That makes life slightly easier for businesses that only operate in one jurisdiction. It's trickier for those with (or planning) a presence across multiple geographies.

This year, Indonesian, Italian and Polish National Identity Cards were the most frequently attacked. In fact, five of the top ten most attacked documents were National Identity Cards. This is because documents not intended for international travel typically have fewer security features than the international equivalents, like passports or driving licenses. It's also because the design of some of these documents is quite outdated - fraudsters have had ample time to familiarize themselves and find the best forms of attack.

For multinational businesses, it's worth considering whether ID verification methods need to be adjusted to different markets to better manage risk.

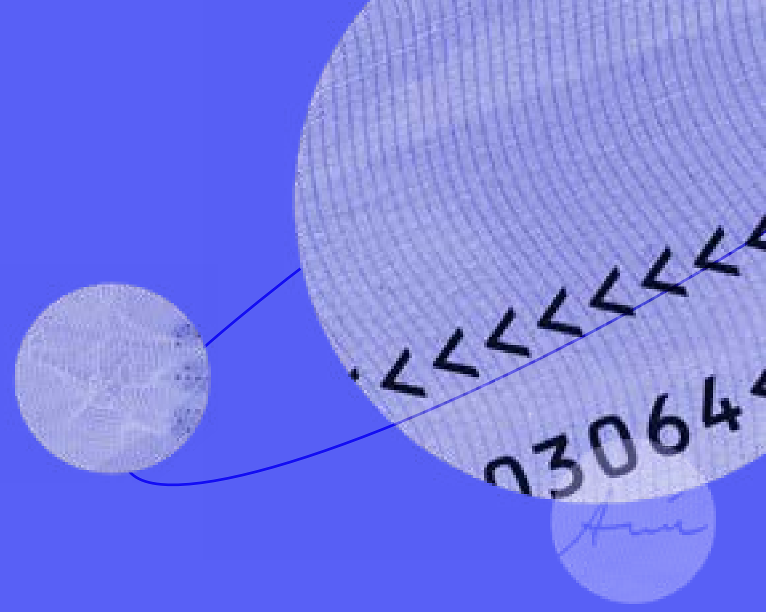
Most attacked document types



Counterfeiting is the most popular method of ID attack

This year, we saw a significant increase in physical counterfeit documents, which accounted for over 90% of all ID fraud. But since fraudsters adapt their technique according to their target, this isn't necessarily representative of the wider market; it reflects our client profile.

We see more physical fraud because so many of our clients use our native Software Development Kits (SDKs). Our SDKs provide drop-in screens and tools to help clients seamlessly integrate verification processes into native mobile apps. The SDKs require users to take a live capture of their document—so they can't just alter an image and upload it. This data shows we're making life harder for fraudsters, who have to fully physically recreate documents. It's a far less scalable form of attack. Other businesses whose ID verification engines don't include these SDKs have less protection, and would likely see more balance between the four attack vectors.



90%

of all ID fraud this year was through physical counterfeit documents

Fraudsters don’t just use one mode of attack; they adapt their techniques to take advantage of the specific flaws in a system

Most used techniques for ID fraud

🟦 🟦

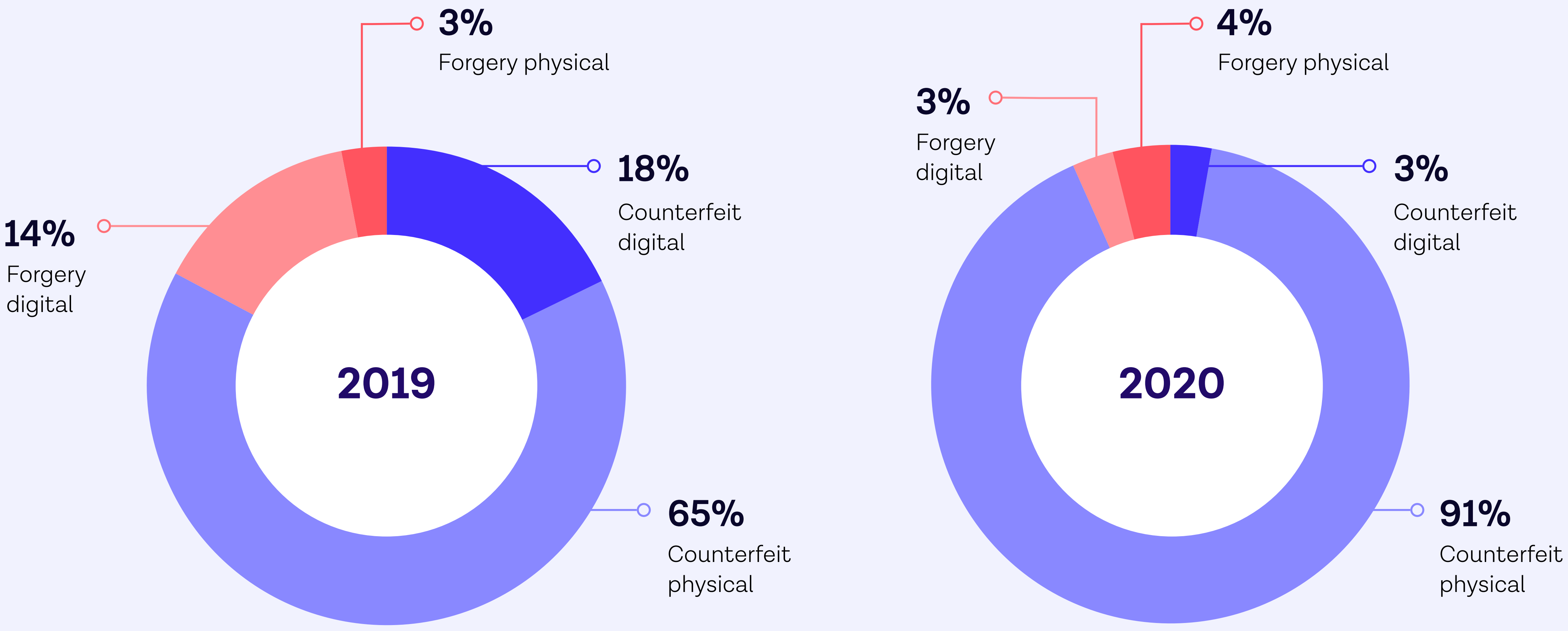
Counterfeit documents

A counterfeit is a complete reproduction of an original document.

🟥 🟥

Forged documents

Forgeries are original documents that have been altered. Changing even a single digit on a document can create a completely new identity.



Most fraudsters miss the detail on data

Fraudsters switch up their techniques. There are lots of different ways to commit document fraud, and businesses need to be able to catch all of them.

As in 2019, we found that most fraudulent IDs fail on data validation. This is a relatively unsophisticated type of attack and maps on to our other findings, which suggest there are more ‘unprofessional’ fraudsters in the market.

ID fraud technique failures

🟦

Data validation fail

Checks a document has valid data in all the correct places.

🟥

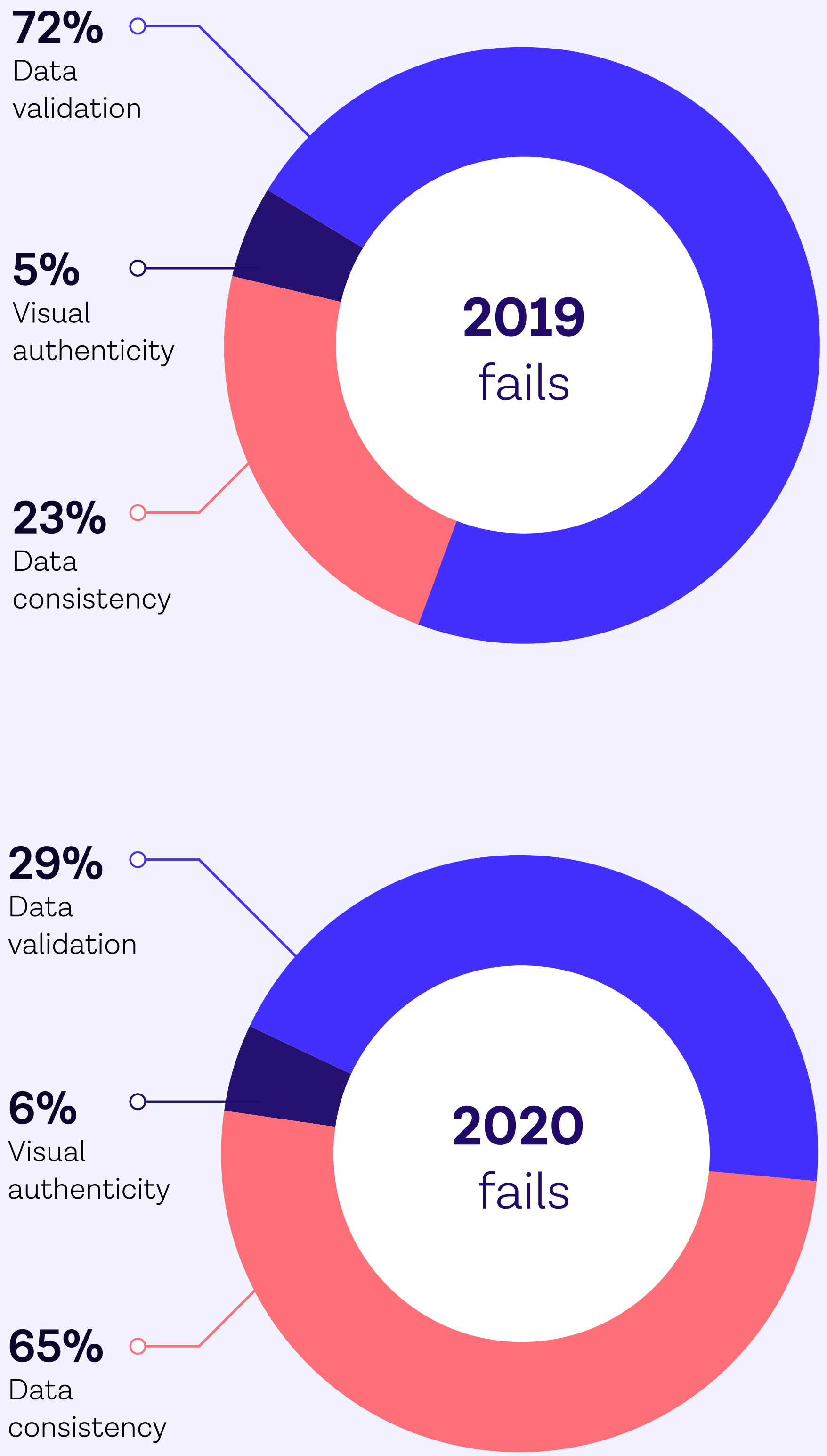
Data consistency fail

Checks data is consistent across all areas of a document. Many documents repeat data in complex ways.

⬛

Visual authenticity fail

Where visual security features have been compromised, font anomalies are present, or a photo has been tampered with.



Biometric fraud is a developing landscape

Due to the ubiquity of stolen personal data, many clients are choosing to layer biometric checks on top of document checks to have the best chance of rooting out identity fraud.

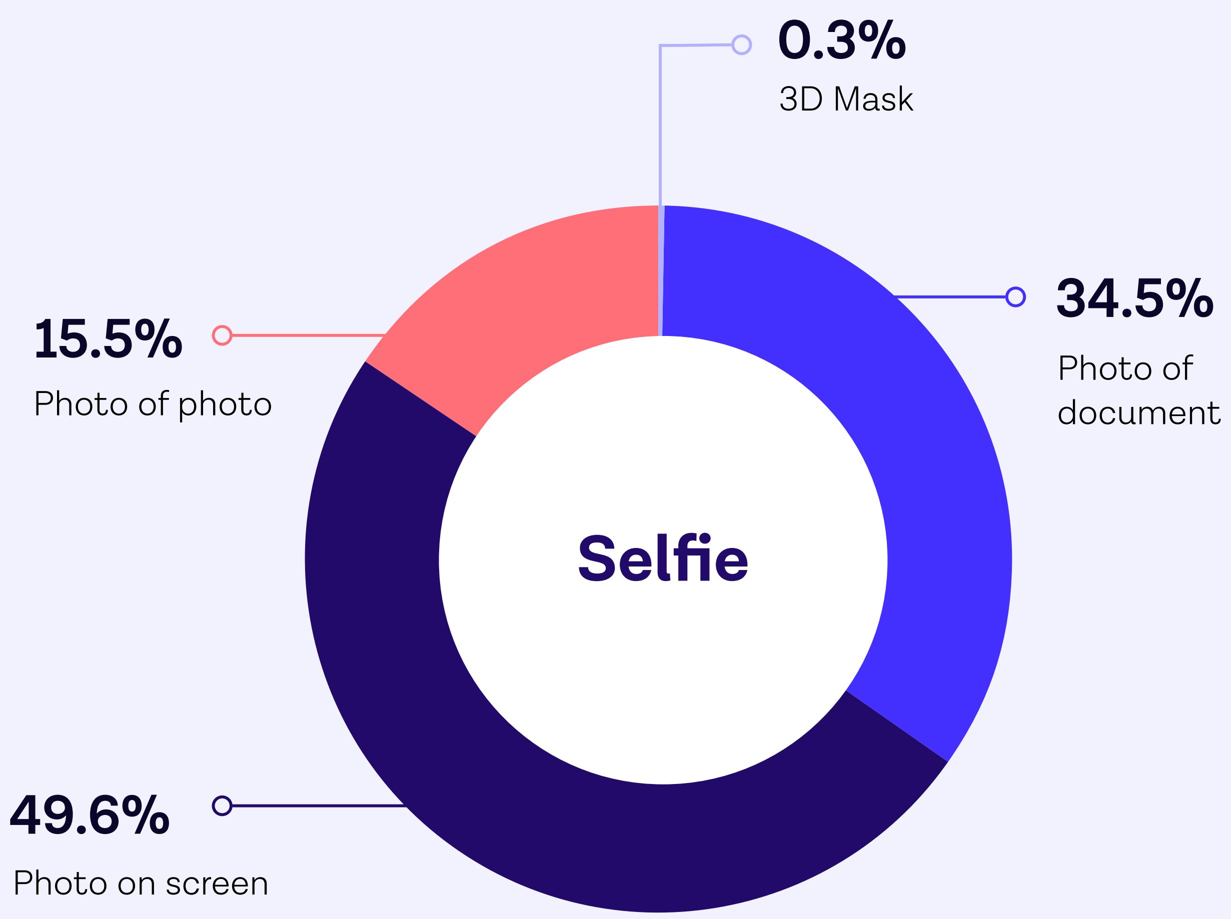
We offer two biometric products. Our Selfie product asks a user to take a static image of their face, and compares it against the photo in their identity document to ensure they are the rightful owner, and that they are physically present at the time of capture. It's a passive form of liveness detection that looks at the image in a single frame, analysing the textures of the photo and various additional signals.

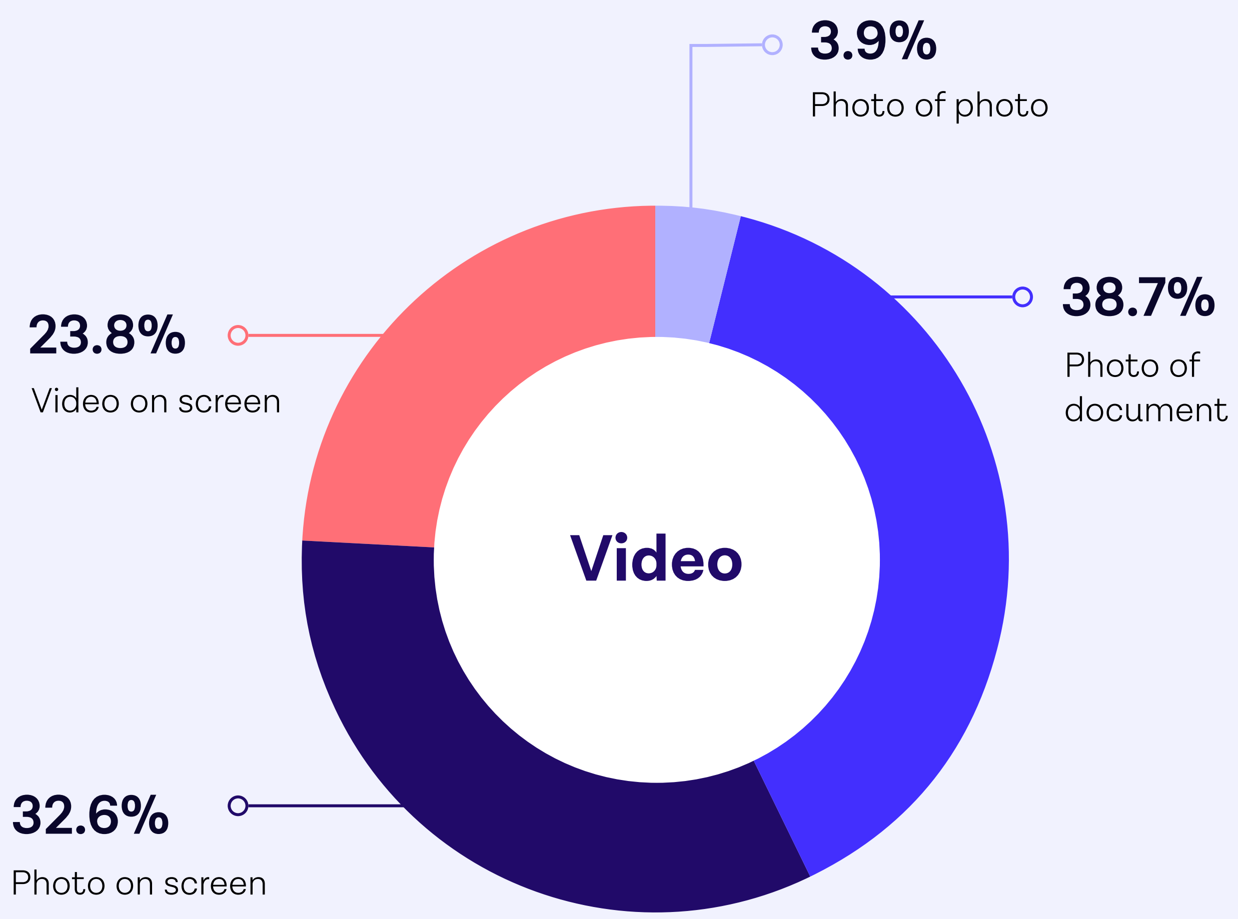
Our Video product adds an additional layer of security by asking the user to record a video where they perform two actions: reading randomized numbers and turning their head. It's an active form of liveness detection that captures several frames, analysing textures and determining lip syncing.

Our data shows that when it comes to biometric fraud, the simplest techniques are currently the most commonly-used. Fraudsters typically attempt to spoof biometric protections by taking a video or photo of a photo, document or screen rather than their own face—attempting to claim document ownership without being physically present on camera. However, instances of more complex techniques suggest that biometric fraud is a developing field, as fraudsters become more confident with the technology.

Biometric fraud is a developing landscape

ID fraud flagged for selfie and video products





Deep dive

Deep dive

Four emerging trends in biometric fraud

Biometrics are becoming increasingly popular in the fight against identity fraud. Document verification adds an additional layer of security to database checks, ensuring that the person presenting identity information really owns it.

Photo biometrics add a layer on top of that, by matching a document to a face, with a passive approach to liveness. And active video biometrics are even more robust. They ensure that not only face and document match, but give higher assurance that a person is legitimately live and present than a selfie.

But biometrics aren't foolproof, and enterprising fraudsters are constantly devising new ways to outsmart them. As with documents, most biometric attacks are still rudimentary, and relatively easy for intelligent identity verification systems to detect. Others are more challenging. These are the four most common types of biometric attacks we currently see.

Spoofs

2D and 3D masks

Replay attacks

Coercion

Spoofs

Our biometric products ask users to take a picture of their identity document and either a picture or video of their face, and then matches the two.

Usually, fraudsters try to 'spoof' the system by taking a video or picture of a picture, document or screen, and submitting that as their biometric. We're able to catch these attacks by analyzing the construction of the image, including textures and shapes. Our Video product uses active liveness, and so is able to catch more sophisticated spoofs. Our Selfie product catches the most common spoofs using passive liveness, and is less frictional for users.

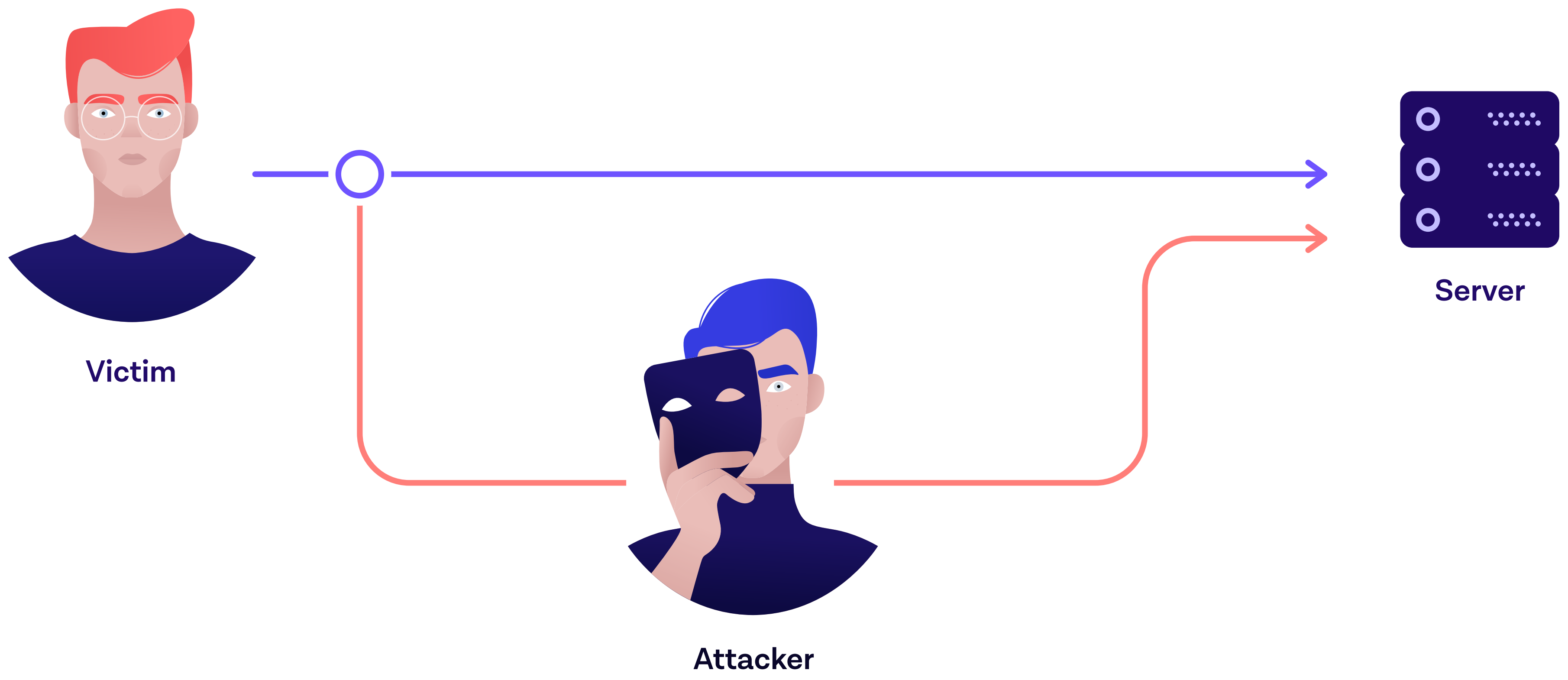
2D and 3D masks

The next step up from taking a photo of a photo is to use a mask. Fraudsters commonly use 2D masks against our video product: they simply print out a photo of the victim's face and cut eye holes in it.

Again, this is quite easy to detect. Our algorithms are able to identify the textural differences between masks and live human faces. 3D masks are more sophisticated, requiring fraudsters to go to some length and expense to create silicon replicas of victims' faces. Unsurprisingly, we see very few of these.

Replay attacks

Replay attacks are becoming more common as a cheaper and easier alternative to 3D masks. Replay attacks can happen physically or digitally, and involve the same false information being resubmitted repeatedly.



Digitally, there are three main ways to perpetrate replay attacks against our biometric products. Fraudsters can either a) circumvent the device camera to insert a stolen or deep fake video, b) infect the device with malware to interfere with the data being sent or c)attempt to attack the API directly, and send fraudulent signals there without needing to go via the user's device. Replay attacks are more common on desktop than on mobile because desktops are more vulnerable to malware and have more attacks vector. What we see most often is software being used to go around desktop webcams and inject malicious biometric signals.

Coercion

Coercion requires no technical expertise at all. Instead of stealing an identity, fraudsters simply coerce victims into opening legitimate accounts, and then use them for illegal activity. Coercion is a growing concern because it's very difficult to detect.

It requires determination of intent, which can be challenging for humans, let alone automated solutions. Typically, coercion victims aren't appearing in biometrics tests with a gun to their head. Sometimes, there might be another person in shot – but this could just as easily be a friend helping them out with the tech. It's a difficult and developing problem that businesses will need to be aware of.

Tips

rités compe
ort
toridades compete
/ Forbeholdt de pas
Vermerke
ου είναι αρμόδιες για τ
pages reserved for issui
daráis eisiúná
tà
te instanties
des competentes
Varattu passin
ndighet.

What to watch out for in 2021

Identity fraud isn't going anywhere. Over the last few years, fraud rates have climbed steadily as data breach has followed data breach. By now, over half of businesses have been hit by fraud, at a cost of $42 billion.[7]

Thanks to the disruption caused by Covid-19, that trend is accelerating. And the bad news is that it's going to keep gaining pace over 2021. With so many digital transformation projects underway, the market is likely to remain volatile for some time. That gives fraudsters more opportunities to make and scale successful attacks against vulnerable businesses.

[7] Source: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

One area where we expect to see significant activity over the next year is synthetic identity fraud

Synthetic identity fraud[8] combines real information (like a stolen Social Security Number) with fake information (like a fake name) to create a new identity. This identity is then used to apply for credit online.

The application will usually be rejected by credit bureaus, as the synthetic identity has no credit history – but the application alone means it now has a credit file. The synthetic identity can then be used to make further credit applications until one is accepted, typically by a high-risk institution. There, synthetic fraudsters can build a credit record that eventually grants them access to other, more credible (and more valuable) institutions.

Synthetic identity fraud is likely to increase thanks to the availability of stolen personal data, which is easier and cheaper to access than ever before. The recent hack of the US Census[9] means that now, virtually every adult's personal information is available to buy. That means database checks alone are worse than obsolete, and businesses without robust document and facial checks will struggle to keep synthetic fraud at bay.

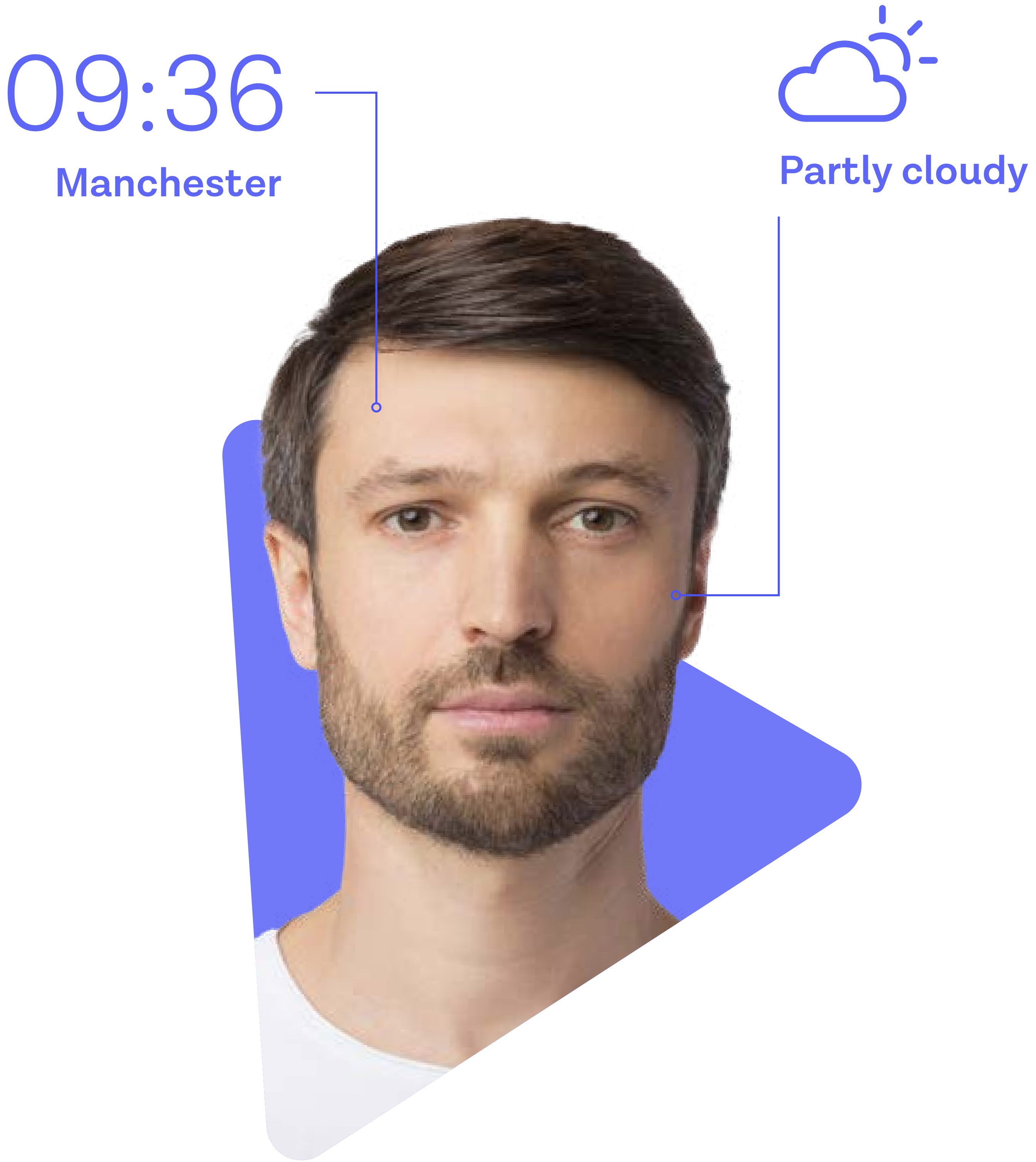
8. Source: https://onfido.com/resources/blog/what-is-synthetic-identity-fraud
9. Source: https://www.techradar.com/news/major-data-breach-exposes-database-of-200-million-users

The continued development of biometric defenses will be a priority for businesses and providers

As deep fakes and replay attacks start to happen more frequently, businesses will need to come up with creative ways to cross-reference and verify identity signals. One way to shore up fraud prevention measures could be to match biometrics with data from the user's device.

There's potential to use other device information (time, GPS, accelerometer, barometer, metadata, browser information, etc.) to support fraud detection, subject to receiving the user's consent where required.

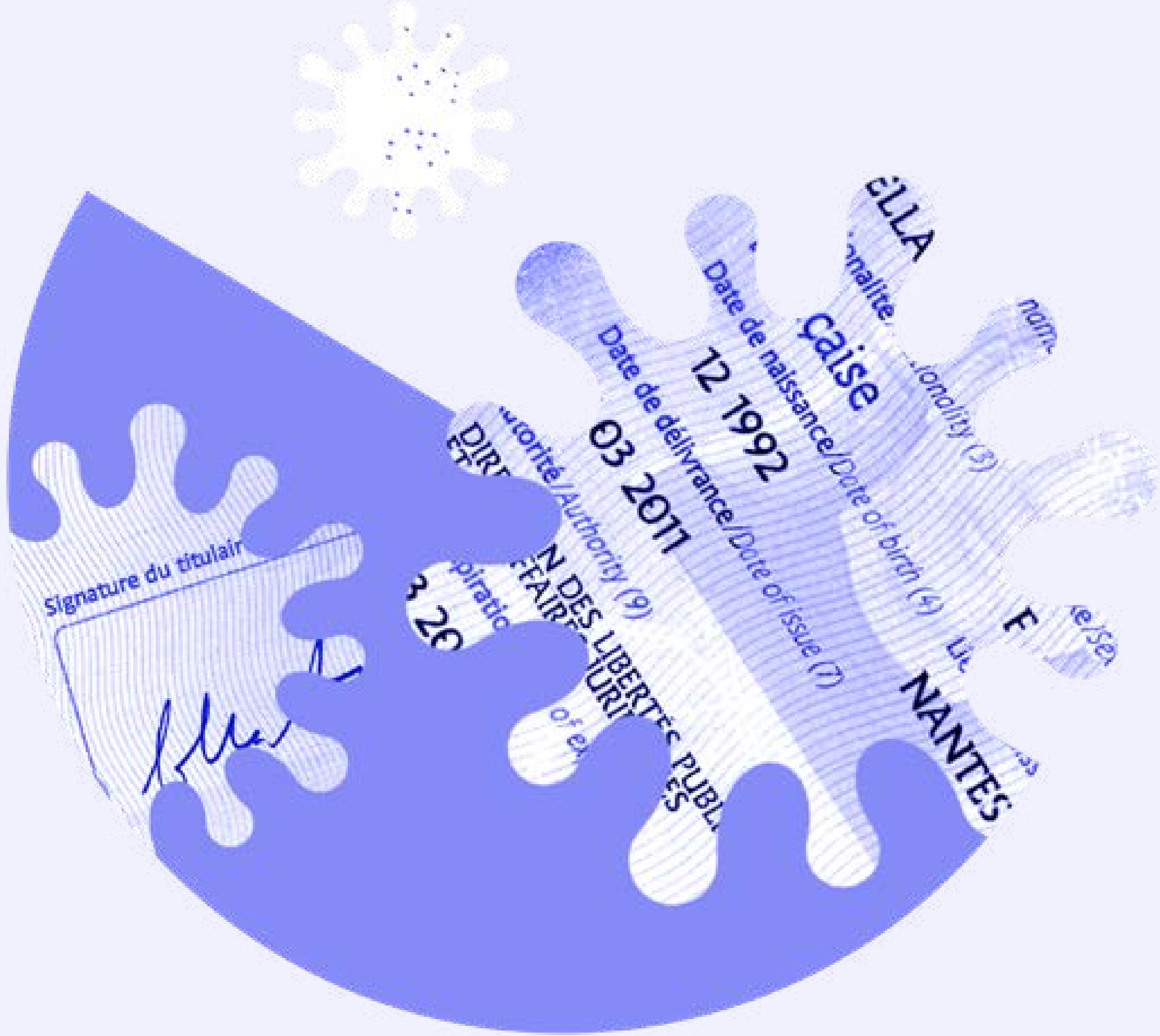
Comparing something like time of day with the amount of light in a selfie could help determine whether an image is likely to be fraudulent or not. Enhancing biometric signals with device telemetry could make life very difficult for fraudsters. It's a developing technique, and one we expect to see gather pace over the next year.



If 2020 has shown us anything, it's that businesses can't always predict what's around the corner – so they need to be prepared

Some are already taking this on board.

We've seen increased demand for identity verification services during the pandemic, especially from Financial Services. Many are taking this time to proactively assess their tech stack and ensure it's fit-for-purpose in an evolving risk landscape. It's a wise move; businesses across all industries would be smart to follow suit.



Best practice

How to strengthen your ID fraud defenses

Find solutions that can dynamically adjust to the changing risk landscape

Layer up identity verification measures

Recalibrate your friendly friction threshold

Be aware of fraud across your customer lifecycle

Best practice

How to strengthen your ID fraud defenses

Find solutions that can dynamically adjust to the changing risk landscape

This year has shown us how surprisingly and dramatically the market can change, opening up new routes of attack for fraudsters. Working with anti-fraud vendors that can dynamically adjust to the market will ensure your business is as well-prepared as possible.

Not all fraud is created equal. The majority of fraud attacks are ‘easy’; fraudsters find one flaw in your system and abuse it repeatedly until you shut it down. Then they move on. But as sophistication increases from “medium” to “hard” fraud, you need to be doing more to deter them from attacking your system in the first place.

Onfido’s hybrid approach helps with this. By using a mix of manual and Machine Learning-based checks, we’re able to keep pace with fraudsters and keep them out. Neither purely human nor purely automated systems are able to respond to the changing risk landscape and recalibrate as quickly. Businesses using them are likely to be caught out again when the next crisis hits.

Best practice

How to strengthen your ID fraud defenses

Layer up identity verification measures

It's been apparent for some years that businesses can no longer rely on data alone to verify identities. That's now been validated by Gartner.

In their "Market Guide for Identity Proofing and Affirmation", they suggested that a lot of knowledge-based verification methods are now "something you-but-not-only-you know". Security information like your mother's maiden name or first car can be easily gleaned from social media, and sensitive PII is available for sale on the dark web. Database checks alone no longer cut it.

If you're still solely relying on background signals, consider baking in document verification to make your defenses more robust. If you're already using document verification, add in biometrics. They'll help to ascertain the real identity of those accessing your platform, and deter fraudsters who don't want to put their face to a name. And for the most sophisticated fraud, consider layering on additional signals such as Onfido's Known Faces to spot when fraudsters are trying to 'brute force' your system by submitting the same illegitimate credentials again and again.

10. Source: onfido.com/landing/2020-gartner-market-guide/

Best practice

How to strengthen your ID fraud defenses

Recalibrate your friendly friction threshold

Anti-fraud processes inevitably add friction into your user experience. That's not always a bad thing. 'Friendly friction' keeps your platform safe: it's just enough to keep fraudsters out without getting in the way of legitimate users. But it's a difficult balance to strike, and has now become even harder.

Businesses that have recently transitioned online need to meet customer expectations of a very slick, low- or no-touch experience. But they also need to protect themselves against exponentially increased risk. Their friendly friction threshold will need to be adjusted accordingly. The best way to approach this is to keep it proportional. Users are happy to put up with more security measures for something that's valuable to them, like protecting their bank accounts. As we discovered in our research on customer attitudes towards digital identity, they're less happy to do it for things like retail accounts, which aren't as sensitive.

Ultimately, it's up to businesses to decide what risk level they're comfortable with. Think about whether you need to catch all fraud (and potentially keep out legitimate users), or are happy to let in a minority of bad actors in order to improve the customer experience for the majority. Establish your risk appetite to ensure you're asking the right questions when evaluating anti-fraud providers.

How to strengthen your ID fraud defenses

Be aware of fraud across your customer lifecycle

The other way to ensure friction stays 'friendly' is to think about where it occurs in the customer lifecycle. It doesn't make sense to ask someone if they're a fraudster when risk is low – when they've just given you their email address, for instance. Instead, try triggering identity verification and fraud checks when they're closest to value, like when they're about to activate their card.

Fraudsters don't just want to access your products and services at onboarding and registration. The rise of phishing scams and impersonation attacks later in the customer lifecycle, such as fraudsters falsely initiating "account recovery" requests, means that you need to be more vigilant. If you're not authenticating customers against their initially verified identity later in their journey with your product, you could be exposing yourself to fraud. To re-authenticate users, you need to ask for something that's uniquely theirs. A selfie can be matched against the document used at registration in seconds, so there's very little impact on their experience. By anchoring a customer's account in a real, genuine identity up front, the process of gatekeeping against fraud later in their lifecycle becomes much easier.

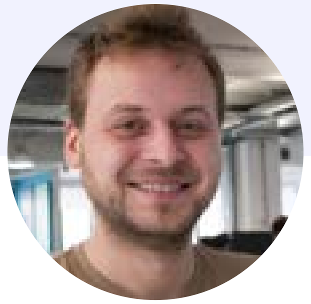
Authors

Michael Van Gestel

Head of Global Document Fraud

A leading expert in ID Document security and fraud, Michael heads Onfido's Global Document and Fraud Strategy Team and plays a central role in Onfido's product development strategy.

Prior to Onfido, Michael worked as a Document Expert and international trainer at the Royal Marechaussee and several global document checking and referencing companies.



Dimi Radu

Senior Document Research Specialist

One of the first employees at Onfido, Dimitrie has held a variety of roles across analytics, operations and technology, playing a central role in developing Onfido's identity verification process.

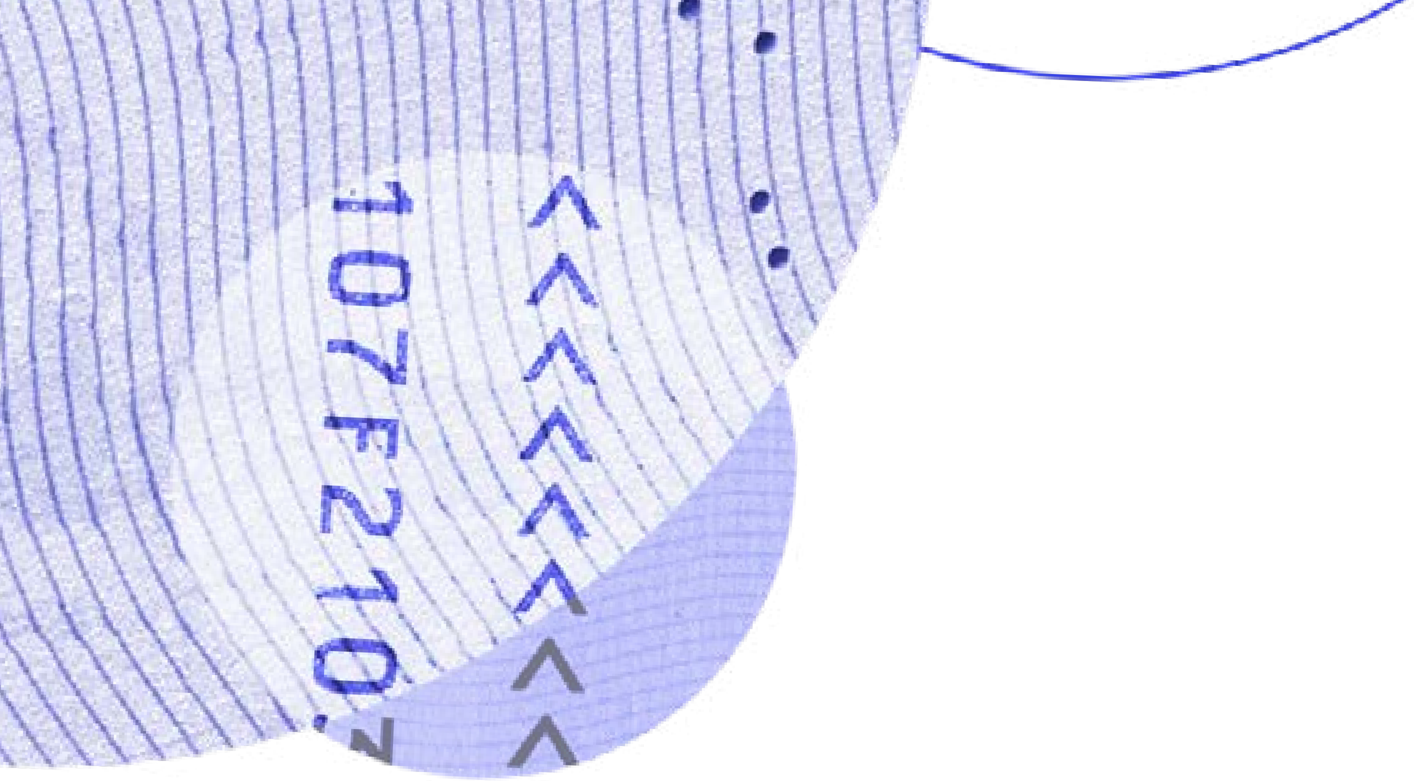
He is now responsible for document fraud research, testing, training, and implementing product enhancements together with the machine learning teams.

Giulia Di Nola

Biometrics Product Manager

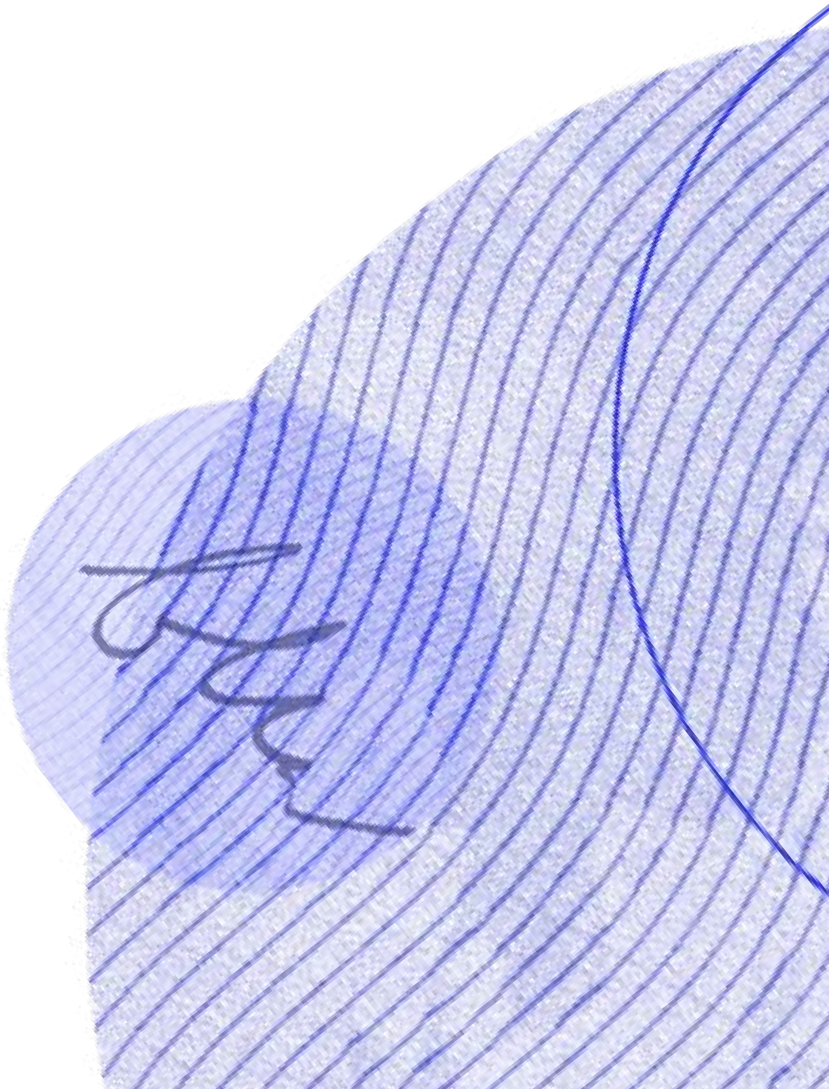
Giulia's background is as a Product Support Engineer. She joined Onfido in 2016, working closely with our global clients to understand what they need from identity verification solutions, and helping them troubleshoot fraud on the ground.

Now, she guides strategy and development for our line of ground-breaking biometrics products. Prior to joining Onfido, Giulia led Customer Support Engineering teams at graphics, vision and AI specialists Imagination Technologies and Evodevo.



Want to know more about fraud trends and how to protect your business against them?

Get in touch



onfido | Real Identity