Signicat

The Battle Against AI-driven Identity Fraud

Growing awareness, increasing threat, but confusion and inaction persist

Signicat in partnership with consult hyperion

Contents

Foreword from Consult Hyperion 3

Introduction - Sophistication at scale 4

Executive summary - The inflection point for AI-driven identity fraud 5

The state of fraud today 7

Awareness of the use of AI to enhance fraud 10

How big is the problem of AI-driven identity fraud? 11

The rise of deepfakes? 12

Are organisations prepared to tackle AI-driven identity fraud? 14

The future of AI threat prevention 16

Conclusion 18

Mitigating AI-driven identity fraud 19

Methodology 24

Glossary of terms 24

Foreword

David Birch
Global Ambassador

Steve Pannifer
CEO

from Consult Hyperion:

The power of AI is undeniable. Within little more than a year it has transformed how we think about the digital economy – accelerating us towards a future with unthinkable levels of automation. AI will bring substantial efficiency gains into all parts of the economy. However, it will also present new threats as bad actors learn how to use the technology for their criminal purposes.

The impact of AI on financial crime is yet to be realised but be in no doubt, there will be an impact. On the positive side, advances in AI will enable better detection and prevention of fraud. At the same time, it is inevitable that fraudsters will exploit the technology to further industrialise their activities.

The potential for AI to be able to subvert identity related processes is particularly concerning. Identity management sits at the heart of financial crime prevention. If it can be undermined then fraud will explode. It is essential that firms understand the threat of AI-driven identity fraud and have a sound strategy to mitigate it. The question is how prepared is the industry for this potential onslaught?

To understand this question, Signicat commissioned a survey of industry practitioners across Europe. The responses show that whilst firms have some appreciation of the threat of AI to their identity systems, the complexities and nuances are much less understood.

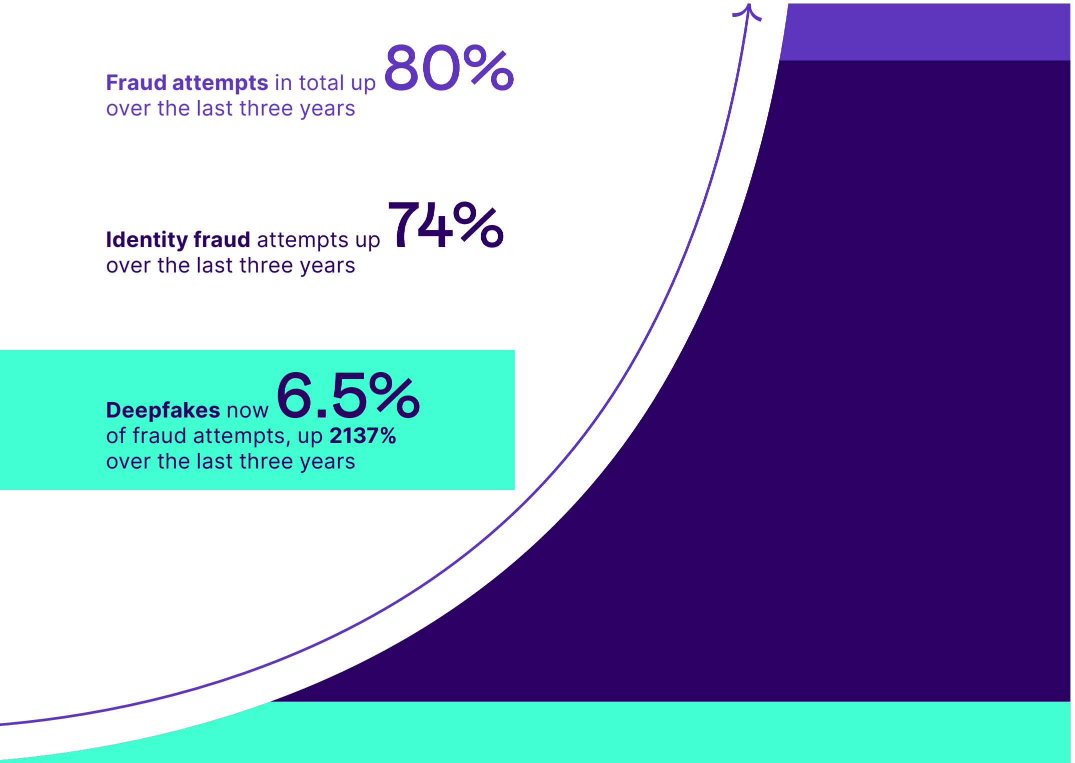
It should be no surprise that the levels of understanding across the industry are mixed. The fraud risks to financial services are changing rapidly. Reported fraud data looks backwards rather than forwards and so practitioners need to rely on anecdotal evidence to understand what is happening now. Perhaps most importantly, AI skills often sit outside the organisation. While machine learning underpins many of the fraud systems employed today, often those capabilities are provided through third-party vendors who bring the necessary specialist and scarce data analytics skill that underpin AI.

It is essential that financial firms have a robust strategy for AI-driven identity fraud. Identity is the first line of defence. Ensuring that identity systems are able to resist and adapt to ever changing fraud tactics is essential, to protect legitimate customers and ensure the reputation of the service.

Introduction - Sophistication at scale

Businesses and governments are struggling to cope with the sheer volume of fraud they have to face. Payment fraud alone costs merchants $38bn globally, and one analyst prediction says this will increase to $91bn by 2028—100 times as much as ransomware. The rules around fraud refunds are also changing, with the UK's new Payment Services Regulation and the EU's proposed PSD3 rules giving customers more rights in some cases of impersonation and Authorised Push Payment (APP) fraud.

Signicat's real-world data has shown an increase in attempted fraud



Fraud attempts in total up **80%** over the last three years

Identity fraud attempts up **74%** over the last three years

Deepfakes now **6.5%** of fraud attempts, up **2137%** over the last three years

Right now, fraudsters have a choice. Either they target victims at scale with low-effort techniques such as generic phishing emails, or spend far more effort on manipulating a smaller number of victims. Taking the time to ensnare someone in a romance scam or to building a convincing deepfake may be worth it when the reward is sufficiently high. But what happens when technology can be used to automate these high effort attacks? What if criminals no longer need to make this choice between scale and sophistication?

AI is driving this change. It has the potential to make fraud easier and more accessible. For example, AI will enable fraudsters to construct more authentic CEO fraud emails. It will enable them to generate fake document images with minimal effort. And, no doubt, they will find other ingenious ways to use the technology. Many of these types of fraud used to take a great deal of time, skill, and experience to carry out successfully. With AI this is no longer true.

But AI is not all bad. It can help prevent identity fraud by analysing vast amounts of data to detect patterns of fraudulent activity, enabling swift identification, and reducing the number of false positives, particularly as part of a layered defence.

Use of AI in identity fraud is an underexplored area, whether that's using AI to forge identity documents, create synthetic identities, fool people with deepfakes—or detect these fraud attempts.

> *Signicat presents the first study into how organisations across Europe are battling the growing threat of AI-driven identity fraud. It asks those who are fighting back against fraud across banks, insurance providers, payment providers and fintechs about their experience, how AI is changing fraud, and if they are prepared to fight it.*

Executive summary - The inflection point for AI-driven identity fraud

76% of decision-makers believe **fraud** is a bigger threat than three years ago

68% of decision-makers believe **identity fraud** is a bigger threat than three years ago

60% of decision-makers believe **eID fraud** is a bigger threat than three years ago

66% of decision-makers believe **AI-driven identity fraud** is a bigger threat than three years ago

AI-driven identity fraud is the use of AI to support or conduct identity fraud, such as the creation of false documents or when used to steal another identity.

eID fraud subverts national digital identity schemes such as Bank ID in Norway or iDIN in the Netherlands, either by taking over an existing account or creating a false identity.

Are we at an inflection point in the battle against AI-driven identity fraud?

Fraud has increased dramatically over the last three years, but there are subtle changes in the most popular types of fraud. With fraud that looks to steal or subvert identity, there is a shift towards more sophisticated fraud types, such as deepfakes. The rise in AI-driven identity fraud confirms this trend. AI is making sophisticated fraud easier.

It is not yet making it more successful—at least, not yet. Success rates for fraud attempts, both AI-driven and not, have remained steady over the last three years.

And that is why we are at an inflection point, the short pause before huge change.

AI is about to enable more sophisticated fraud, at a greater scale than ever seen before. Fraud is likely to be more successful, but even if success rates stay steady, the sheer volume of attempts means that fraud levels are set to explode.

There has been a shift in the last three years, from creating new accounts using forged credentials, to compromising accounts that already exist. Account takeover attacks are the most popular type of fraud, often compromising weak or reused passwords. Deepfakes, often used to impersonate the holder of an account rather than creating a new or synthetic identity, are far more popular than they were. Fraudsters are happy to evolve and attack where they see vulnerabilities.

Organisations are unprepared for the threat. They do not know what techniques and technologies will help them the most, and their plans to fight back are just that: plans, with implementation timescales mostly in the next twelve months. Even more worrisome is that organisations report that the deck is stacked against them: they lack budget, expertise and time.

To begin to fight back, they need to take an approach to security where systems work together to defeat fraud without raising too many false positives. Using multiple technologies in combination makes the job of the fraudster exponentially harder, as they need to beat each technology at the same time to be successful.

Organisations also need to integrate their own defences using AI that can orchestrate these systems and find the patterns that will indicate fraud. Fraudsters and the organisations they seek to defraud are now in an arms race, and the side that fails to keep up will lose.

But most of all organisations need to do more than recognise that the problem exists, they need to better understand the details and how it can be tackled.

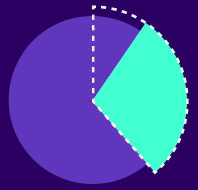
Key findings at a glance

1. **Account takeover** is the most common fraud type for **B2B organisations**.

2. Three years ago, AI was mainly used to create synthetic identities and forged documents. Today, it is widely used for **deepfakes and social engineering attacks**.

3. Over the past three years, **deepfakes** have become the **most prevalent threat in eID fraud**.

4. An estimated **42.5%** of detected fraud attempts use AI, with **29%** of them considered successful.



5. The largest increases in deepfake targeting over the past three years have been against **banks, fintechs, and the largest businesses**

6. Fraud decision-makers see AI driving future identity fraud but are **confused** about its nature, impact, and prevention technologies.

7. Fraud decision-makers **lack the resources** to tackle the issue with **necessary speed**.

8. Over three-quarters of businesses prioritise AI-driven identity fraud prevention, planning technology upgrades and budget increases, with **less than a quarter** having started implementation.

□ □ □ ☒

The state of fraud today

David Birch and Steve Pannifer from Consult Hyperion:

Getting a true understanding of fraud is difficult. Fraud statistics are not reported in a consistent and uniform way (although PSD3 reporting requirements should improve this). Some frauds go unreported, for example if the victim is too embarrassed. Where regular reporting does occur this is typically done annually so potentially fraud figures are a year out of date. These issues are exacerbated when the landscape is changing rapidly, creating new opportunities for fraudsters to exploit weaknesses before the industry and regulators catch up. And this is the situation we are in now.

Prior to the market wide implementation of strong customer authentication (SCA), under PSD2, card not present (CNP) fraud was a major problem. Fraudsters could steal card details and because of the lack of authentication in CNP transactions, perform them with ease. The PSD2 regime has now been in place long enough that the effect of stronger authentication controls can be seen in the data. The ECB reports clear evidence of CNP declining for example.

Inevitably, this has caused fraudsters to change their tactics and look for new weaknesses to exploit.

The EBA reports three emerging trends:

- **PSD2 Exemptions**, where SCA is still not a requirement – such as “merchant initiated transactions” and “mail order telephone order” transactions. Inevitably these continue to be a target for fraudsters.
- **Authorised Push Payments (APP)**, where the payer is manipulated through social engineering, is growing rapidly although some countries are being hit harder than others.
- **Account Takeover (ATO)**, where the fraudster may invest time and effort, using a combination of stolen data and phishing techniques, to gain access to a victims financial account and the potential of a significant pay day.

Alongside account takeover we would include mule accounts and accounts created using synthetic identities. So whilst APP scams are initiated outside of the payments system, for example on social media sites, they still rely on accounts of victims that they takeover or control. This is identity fraud.

We asked fraud decision-makers across Europe about how fraud had changed over the past three years.

What are the most common types of fraud you experience?

	Three years ago		*Today*
#1	Card payment fraud	#1	Account takeover
#2	Identity theft	#2	Card payment fraud
#3	Account takeover and Phishing	#3	Malware and Phishing

While we found that fraud has increased overall, some types of fraud have become more popular. Identity theft, a subset of identity fraud where an identity is taken over, is no longer one of the top three types of fraud.

Some types of fraud are increasing in popularity faster than others, such as account takeover and malware. The battle against fraud can be seen as continually changing as fraud prevention improves, and fraudsters change tactics to get around new technologies and fraud prevention measures. One overriding theme we can see here is that fraudsters are looking to compromise accounts that are already in use rather than create new ones.

This trend is true of both B2B and B2C businesses. Despite account takeover generally being seen as a consumer issue, it is actually the most common fraud type for B2B organisations.

What are the most common types of identity fraud you experience?

	Three years ago		*Today*
#1	Account takeover	#1	ID document forgery
#2	ID document forgery	#2	Synthetic ID fraud
#3	Synthetic ID fraud	#3	Account takeover, Deep-fakes and Impersonation

When we look specifically at identity fraud, the most popular types of fraud have remained mostly the same over the last three years, with some slight changes.

The use of deepfakes, where someone is impersonated using a video or voice copy, has had a lot of media attention in recent years. It's not surprising to see it as a new entry to the top three. However, it's perhaps not as new as we think, ranked just outside the top three threats three years ago, though today it's more sophisticated and much better known.

This tracks with Signicat's own real-world experience in detecting deepfake fraud. Three years ago, it was just 0.1% of fraud attempts, and today it is around 6.5%, or around one in every 15.

While most attention is given to consumer deepfake fraud, it is just as common for B2B organisations.

Fraud variance: Not all countries have the same experience of identity fraud, despite having similar regulations, and access to similar technologies.

- Synthetic ID fraud is most prevalent in the Netherlands and Belgium
- Germany reports the highest incidence of ID forgery
- Belgium suffers the least from impersonation attempts
- Norway experiences the most deepfake attacks, but they are less common in Germany, Spain, and the UK

What are the most common types of eID / digital identity fraud you experience?

	Three years ago	*Today*
#1	Account takeover	Deepfakes
#2	ID document forgery	ID document forgery
#3	Synthetic ID fraud	Account takeover and Synthetic ID fraud

Over the last three years, deepfakes have become the most common threat used in eID fraud.

eIDs are effective in preventing fraud, but they will not eradicate it. 60% of organisations stated that eID fraud is a bigger threat than three years ago, compared to 74% saying the same of fraud in general. We can see eIDs are slowing down the increase of fraud, but not stopping it. Fraud decision-makers need to understand that while eIDs are just a big part of the puzzle, they are not a complete solution. AI fraud, like all fraud, targets both systems and people, and if the focus is on fooling a person, eIDs will only be of limited use in prevention.

Deepfakes and digital identity

eIDs are effective against many types of fraud, but fraudsters work hard to subvert the systems designed to stop them. The use of AI makes sampling voices and video to fool people increasingly effective, even if it wouldn't fool a voice or facial recognition system. Someone fooled by a deepfake may be directed to make payments where there is no ID check on the fraudster, only on the person paying, so it will offer no protection. Deepfakes can also help to direct victims to fake eID verification sites to steal logins or as part of a "man in the middle" attack.

Awareness of the use of AI to enhance fraud

AI presents the opportunity for fraudsters to make their fraud attempts more effective and easier to conduct. How has this changed the types of fraud being carried out?

What are the most common types of AI-driven identity fraud you experience?

	Three years ago		*Today*
#1	ID document forgery	#1	Deepfakes
#2	Synthetic ID fraud	#2	Account takeover
#3	Account takeover	#3	Impersonation / Identity cloning

Three years ago AI was being used to create new or synthetic identities, and create better forgeries of documents. The respondents believe it is being used more for deepfakes and social engineering attacks today.

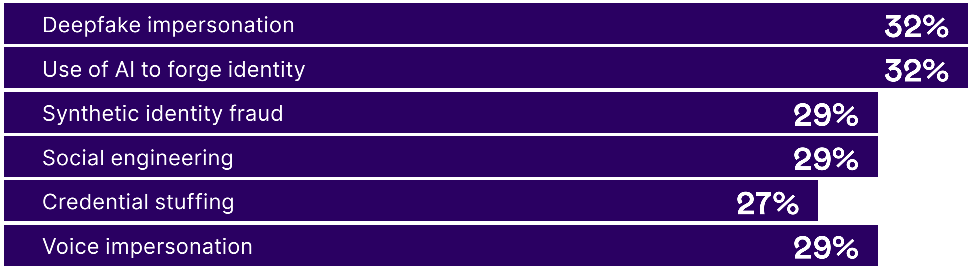
These new uses of AI have been made possible through the significant advancements made in the technology over the past two years.This reflects how AI is changing and its increased sophistication in a short period of time. As well as being used to create static identity documents, it is being used to fool people in real-time over video and voice calls.

Perceptions towards AI and identity fraud

AI is, today, a major driver of identity fraud	73%
AI will drive almost all ID fraud in the future	74%
AI will mean more people fall victim to fraud than ever before	74%

There is, in general, a very high awareness of the problem of AI-driven identity fraud. Most fraud decision-makers agreed that AI is a major driver of identity fraud, that AI will enable almost all ID fraud in the future, and that AI will mean more people will fall victim to fraud than ever before.

Which of these AI-driven fraud techniques have you heard of?



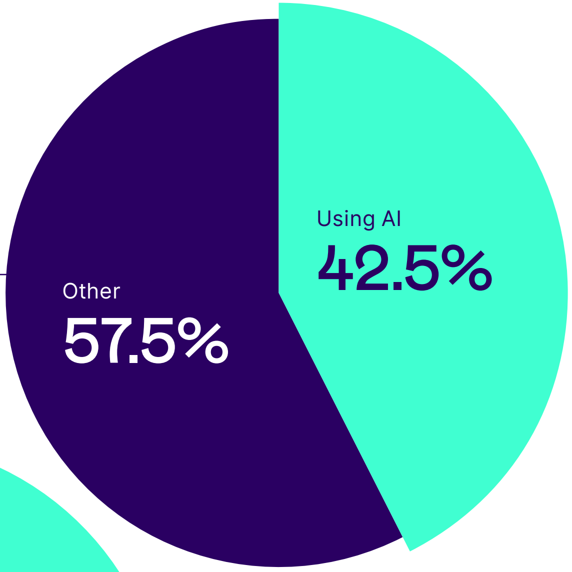
When we dive into the detail, we find specific information lacking. When asked which AI threats they had heard of, no more than a third could say they had heard of AI to forge identity documents, for deepfake impersonation, or for voice impersonation.

This reveals a big disconnect. Fraud decision makers know that AI is a problem, but they are confused when it comes to its exact nature, and how it will impact them.

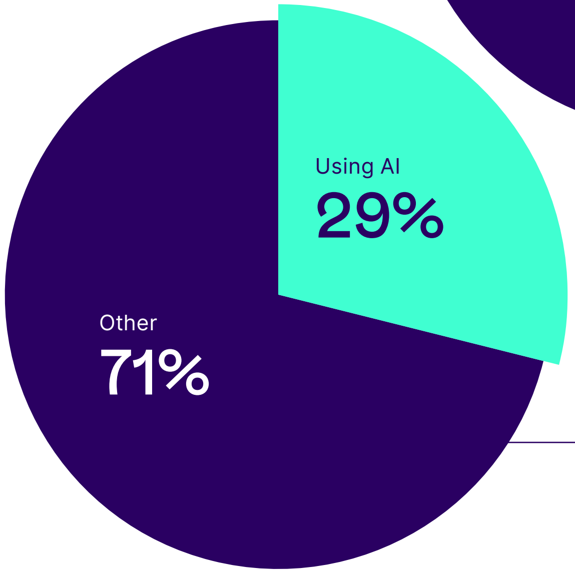
How big is the problem of AI-driven identity fraud?

Fraud decision-makers understand that AI is fuelling identity fraud, and will only get worse. But what is the scale of the problem?

How many fraud attempts that you detect use AI?



How many successful fraud attempts use AI?

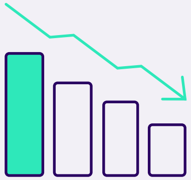


On average, respondents estimated that 42.5% of fraud attempts detected use AI. For some respondents, this was even higher. One in nine said that they estimated AI usage in fraud attempts to be as high as 70% for their organisation. AI is not a future problem, but something that needs to be tackled now.

Respondents also stated that 29% of fraud are "attempts", that is, the fraud attempt initially worked, though it will have been detected later. This number is the same for "completed" AI-driven fraud attempts, also 29%.

AI-driven identity fraud is as effective as fraud using traditional means. As the technology improves it is reasonable to expect that AI-driven identity fraud will become more effective. Organisations are spending billions to stop fraud, and yet a third of all fraud attempts are still successful.

What does this tell us about the use of AI? It is clearly already in widespread use by fraudsters, but it is not yet a runaway success.
As organisation's push back on fraud with better technology and better processes, fraudsters are upping their game with the use of AI.



Revenue loss due to AI-driven identity fraud

Putting a number on the amount of revenue lost to fraud is not easy. Consumers and businesses are not always willing to admit that they have been scammed, and providers may not be willing to reveal the extent of the fraud that they face. Much of the research focuses on specific types of fraud, for example Nilson Report estimates that **$33.45 billion was lost to card payment fraud globally** in 2022, which encompasses many types of fraud, including cards obtained through some form of identity fraud. Sifted.eu cites a report that, in 2020, **identity fraud cost the global economy $5 trillion dollars**—though this will include many indirect costs alongside revenue loss.

Our respondents estimate that, of the revenue loss to fraud, **38% was due to AI-driven identity fraud**. This suggest that, while AI-driven identity fraud is not yet more successful than other means of identity fraud, it is more lucrative and used for more sophisticated, high-value scams.

We are at an inflection point, where AI is being used to assist in fraud attempts but not yet responsible for more successful fraud attempts. This will change as AI becomes more sophisticated and fraudsters make better use of it. The use of AI will mean fraudsters can scale up their operations, and increase the number of fraud attempts they can carry out. Organisations have a very small window of opportunity to start fighting back, before AI tips the balance in favour of the criminals.

The rise of deepfakes?

David Birch and Steve Pannifer from Consult Hyperion:

To unpack the nature and impact of deepfakes, consider two questions:

What is a deepfake in an identity context?

At the most basic level a deepfake is a digital video representation of a real customer. It must:

- Look like the real customer to the identity management system.
- Move and behave like the real customer, in the way that the identity management system requires.

Generative AI will enable the production of increasingly realistic deepfakes. Today that may involve developing the deepfake ahead of time, which may bring the challenge of coordinating the video with user experience being presented. Eventually it may be possible to generate deepfakes dynamically overcoming this issue.

How is a deepfake presented in a transaction?

A simple way to present a deepfake is to place a screen in front of a camera. This should be fairly easy to detect. A more sophisticated presentation would involve injecting the video into a compromised device or app being used to confirm the customer's identity. Video injection will be hard to detect and may allow attacks to be performed at much greater scale – without the physical constraints of real screens and cameras.

The use of deepfakes has received much attention. Manipulated video or voice to mimic someone makes for good TV, but do fraud decision-makers consider it to be a big problem? The earlier results suggest that the technique has grown to be a major part of AI-driven identity fraud. How is that affecting attitudes towards it?

Attitudes towards deepfakes

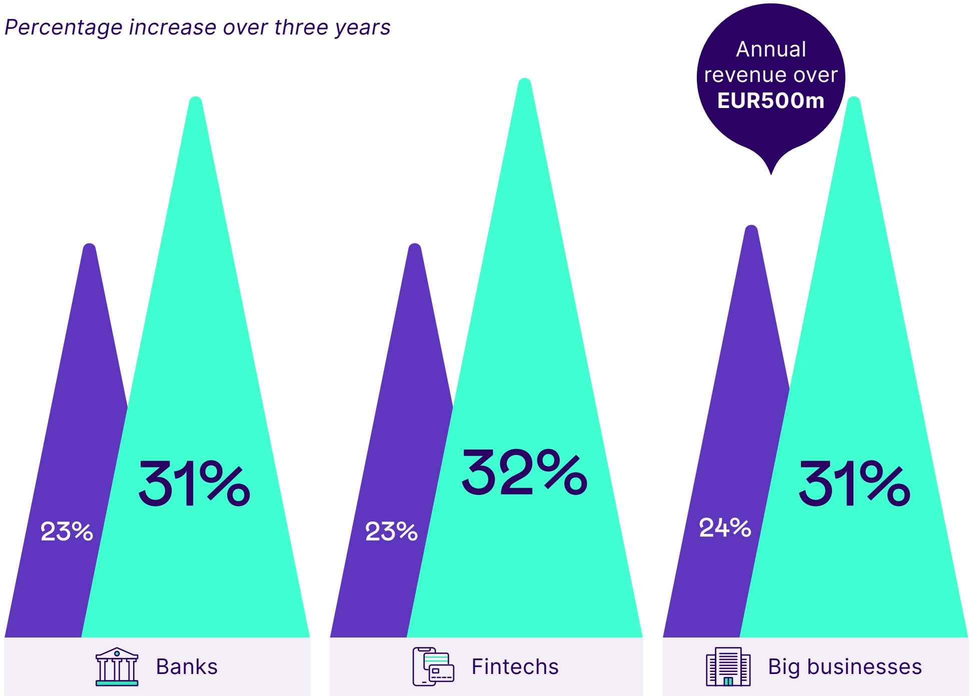
Deepfakes are a common way to perform identity fraud today	77.94%
Human detection isn't enough, deepfakes will require technology to detect	77.45%
Deepfakes will never be convincing enough to fool financial institutions	75.21%

Over three quarters of respondents agreed both that deepfakes are a common way to perform identity fraud today, and that technology will be required to detect it—humans won't be able to do so. This is encouraging. Decision-makers understand that AI is a threat and that they can't be complacent—or do they?

Around three quarters also agreed that deepfakes will never be convincing enough to fool financial organisations, despite the worries around their increased use.

This reveals a lack of understanding, and is, at best, a conflicted picture. Businesses agree that technical intervention is necessary—while at the same time agreeing that financial providers are mostly immune to the problem.

Where are deepfakes targeted?



Percentage increase over three years

This is especially naive when we consider where deepfakes are being targeted. The biggest increases over the last three years are against banks, fintechs, and the largest businesses. These are the organisations likely to have the best fraud prevention technology, and so fraudsters will need more sophisticated techniques to enjoy success. Deepfakes are not yet easy to access and easy to create, and so are being targeted carefully where they can be used for a bigger payout—this, of course, is likely to change as the technology becomes more capable.

Are deepfakes becoming more sophisticated?

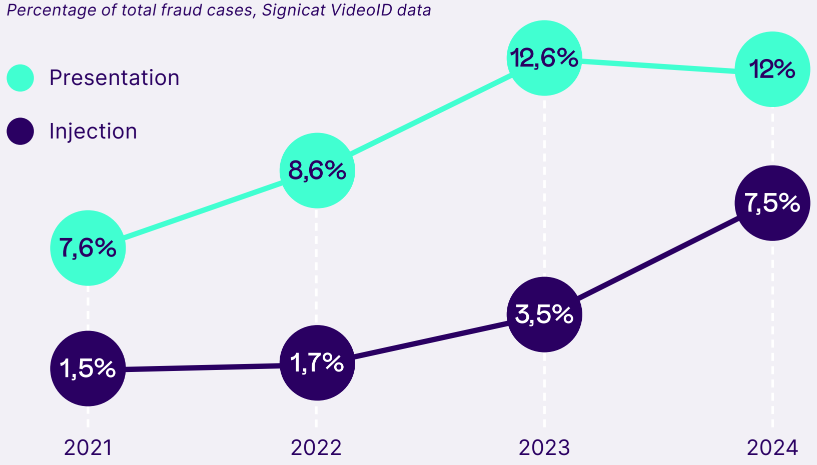
We know that AI can create more sophisticated and convincing live deepfakes of people, but what about how they are used?

We looked at how common presentation attacks are when compared to injection attacks. Presentation attacks include people wearing masks and makeup to spoof another person, but also where the camera films another screen showing a deepfake. Injection attacks are when malware or untrusted input is deliberately inserted into a program, compromising its integrity or functionality. These attacks include the insertion of deepfakes or manipulated pre-recorded videos.

The increase in number of injection attacks, and the plateauing of presentation attacks suggest that deepfakes are not only more common, but more sophisticated in their application.

Evolution of Presentation attacks vs. Injection attacks

Percentage of total fraud cases, Signicat VideoID data



Are organisations prepared to tackle AI-driven identity fraud?

Our examination of attitudes to deepfakes reveals that decision-makers do not fully grasp the impact deepfakes will have on levels of identity fraud. Does this extend to AI-driven identity fraud in general?

We asked about the best defence methods that would prevent AI-driven identity fraud, and the results were not encouraging.

What are the best defence methods to prevent AI-driven identity fraud?

#1 Biometrics

#2 Stronger passwords

#3 In-person interviews

These techniques are a mix of good, ineffective, and a little of both.

Stronger passwords, while good security practice, are not a reliable defence against AI-driven identity theft. They are more effective against attacks that directly target reused or popular passwords, such as brute force dictionary attacks or using passwords stolen in a data breach. In-person interviews would be a good defence against deepfakes, but would be difficult to scale and see resistance from digital native consumers. Biometrics do help, though they are best supported by background signalling such as behavioural biometrics and location data.

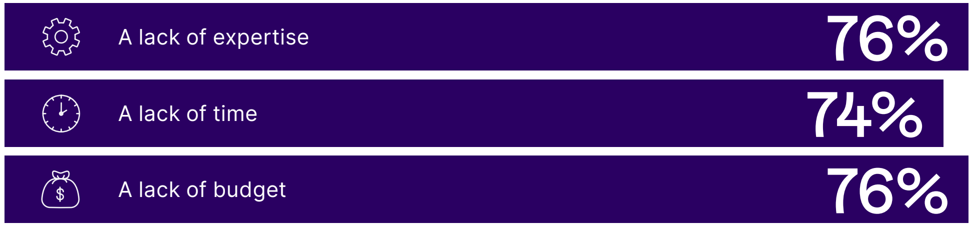
eIDs were seen as the most useful defence in Norway, chosen by 25% of respondents, perhaps understandable given its mature and effective eID programme. However, they were a much less popular choice in Sweden, despite the widespread adoption of eID. And even though respondents were confident in the ability of financial organisations to detect AI deepfakes, in-person interviews were cited as a more popular choice than video interviews.

A better technical understanding?

In general, banks and payment providers suggest stronger passwords are a good defence, while insurers and fintechs advocate for alternative measures. This difference may reflect differing levels of awareness about fraud types, potentially influenced by fintechs' greater tech knowledge and insurers' experience in detecting first-party fraud.

Of course, no single method is effective on its own, and multiple layered methods are necessary to create the best security possible. But there remains confusion about what combinations will create the best defence against AI-driven identity fraud.

Which of these hinder your ability to detect and combat AI-driven identity fraud?



We wanted to pinpoint exactly why organisations are not ready for this sea change in the way fraud is conducted. But there was no single reason: Fraud decision-makers are hampered by multiple barriers: a lack of expertise, a lack of time, and a lack of budget.

Right now, organisations are relying on existing technology to combat a rapidly shifting problem. The impact of AI-driven identity fraud has not yet been fully realised, but that could change very quickly given the rapid development of AI, enabling fraud at a far larger scale.

The future of AI threat prevention

We are at an inflection point of AI threats, and while organisations are aware of the problem, they are hampered by two big problems: they don't know the best ways to prevent AI-driven identity fraud, and lack the resources to tackle the issue with the necessary speed. But there are reasons to be optimistic.

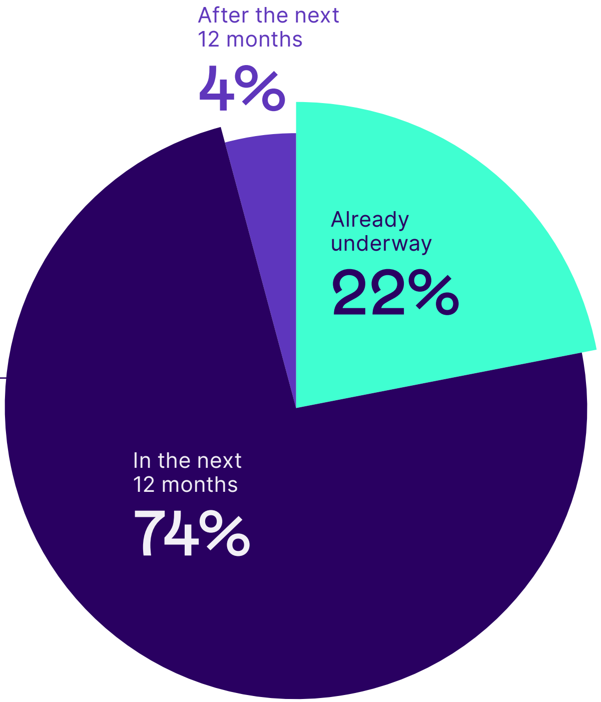
How are you tackling the issue of AI-driven identity fraud?

We have a team dedicated to the issue	78%
We are increasing our budget	77%
We are upgrading our technology	77%

Over three-quarters of businesses have specialist teams dedicated to the issue of AI-driven identity fraud, are upgrading their fraud prevention technology stack, and expect to have more budget to do so.

However, this is not enough on its own to allay concerns. There is confusion about the right methods to prevent AI-identity fraud, so we cannot be sure that the right choices will be made with this investment.

Timeline to implement AI-driven identity fraud measures



Just under a quarter of respondents have actually started implementing measures. Most of the remainder are planning to do so in the next year. Smaller organisations are actually further behind, with only 18% having mitigation in place already.

We already know that decision-makers are behind the curve—AI threats are already here. And we know that the right defence measures are not being prioritised. If organisations want to get ahead of AI fraud, they need to fight back with AI.

David Birch and Steve Pannifer from Consult Hyperion:

Legacy fraud prevention systems often rely on business rules that are defined to address known high risk scenarios. For example, a rule could be defined that if the location of the device does not match the expected location of the user then additional checks should be made. While such rules can help to mitigate well-known common issues, they can be difficult to maintain, especially as the complexity of scenarios increases.

AI technologies and techniques offer distinct advantages over legacy approaches including:

- **Massive Data Analysis:** AI can analyse massive amounts of data in real-time, sifting through transactions, user behaviour, and other details to identify anomalies that might indicate fraud.

- **Pattern Recognition:** Models are trained on historical fraud data, enabling them to recognise patterns and suspicious behaviours that could signal a fraudulent attempt. These patterns can be subtle and evolve over time, making them difficult for humans to detect.

- **Predictive Analytics:** The technology can potentially go beyond simple detection, to predicting when transactions or users are more likely to be fraudulent.

To maximise the potential of AI to fight fraud organisations will need to consider:

- **Data:** ensuring the input data is complete and high quality, to ensure the models are as effective as possible. Pooling data with other organisations (e.g. via fraud prevention vendors) will help identify emerging threats.

- **Tooling:** ensuring a flexible approach so that new models can be introduced as the threat landscape evolves.

- **Expertise:** engaging in-house and third-party expertise, to maintain ownership whilst accessing the scarce specialist skills.

Conclusion

This report reveals a worrying picture.

There is confusion and limited understanding over what AI can do, and the best technologies that can prevent these attacks. While many organisations are planning to invest in mitigating the effects of AI, they are behind the curve.This slow pace of change is likely related to the lack of expertise—how can fraud prevention teams put the right processes in place if they don't know what they are?

It's not entirely bad news. Fraud decision-makers do understand the threat that AI poses in its ability to make identity fraud easier, more accessible, and work at scale. They can detect AI in the attacks they face, and they understand that the problem is only going to get worse.

Unfortunately, there is no silver bullet to stop this problem, it needs to be a combination of effective techniques. Only through implementing multiple technologies and techniques can they defend against fraudsters that are looking to exploit any vulnerability.

In fact, the very technology being used by fraudsters can be used to defend against them: they need to battle AI with AI. AI can be used to detect where fraud attempts are being targeted, can detect patterns that reveal fraud that would otherwise be missed, and cut down on the number of false positives.

To supplement this, there also needs to be education. The rise of AI-driven identity fraud will mean more attempts against systems, but also against people. This means organisations need to prepare their employees and customers not only for fraud that is more convincing, but far more common than before.

Our results do show that AI-driven identity fraud is not yet the runaway problem it could become, but the clock is ticking. Organisations need to act now to recognise the threat and how big it could potentially become, and put in place the combination of solutions necessary to mitigate it.

Mitigating AI-driven identity fraud

The advent of AI means that fraud is, even more than before, ever-changing and evolving. To combat this, fraud decision-makers need to constantly update their knowledge and educate those around them, from the C-level to front-line staff, and of course customers.

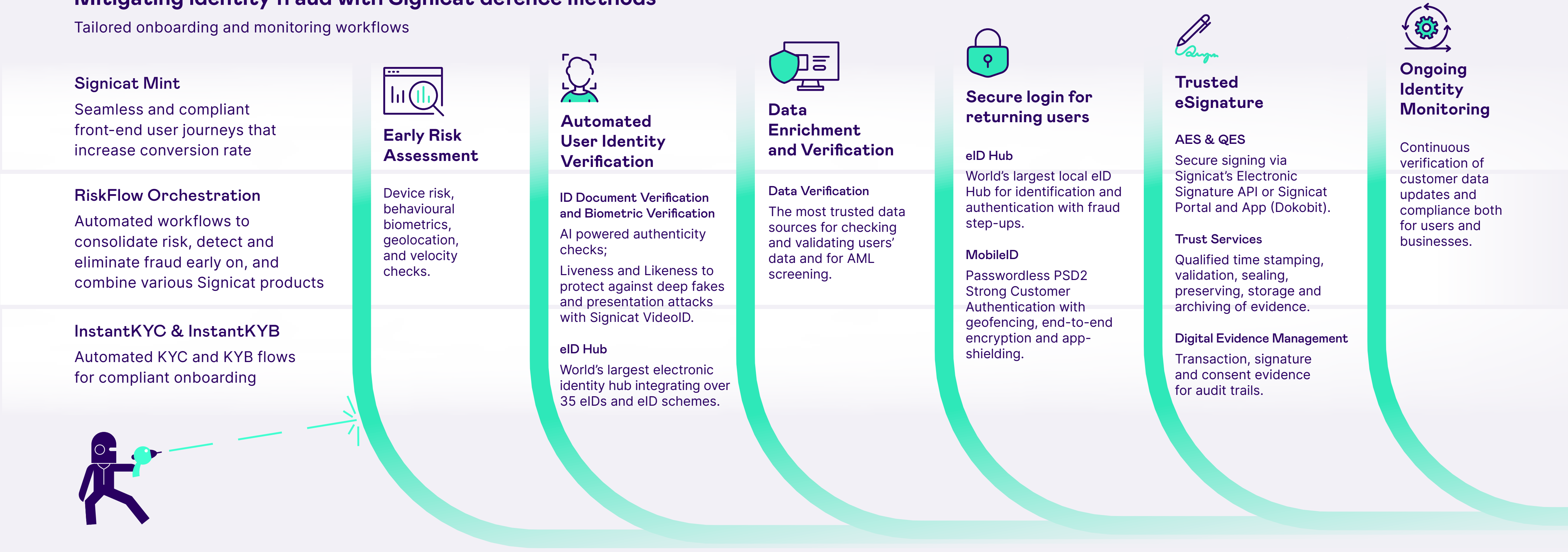
Understanding AI is paramount in mitigating AI-driven fraud. It is important to seek expertise and training to grasp its nuances. Vendors also offer valuable insights as they adapt fraud mitigation technology to reduce AI-related fraud risks.

Digital identity has been an effective weapon against fraud. Given the diverse tactics employed by fraudsters, defence strategies must be multi-layered, covering all vulnerable fronts, from user onboarding to login processes.

Signicat's versatile platform provides tailored solutions ready for deployment. We strongly recommend organisations combine, deploy, and continuously improve their approach to strengthen their defences.

Mitigating identity fraud with Signicat defence methods

Tailored onboarding and monitoring workflows



Signicat Mint

Seamless and compliant front-end user journeys that increase conversion rate

RiskFlow Orchestration

Automated workflows to consolidate risk, detect and eliminate fraud early on, and combine various Signicat products

InstantKYC & InstantKYB

Automated KYC and KYB flows for compliant onboarding

Early Risk Assessment

Device risk, behavioural biometrics, geolocation, and velocity checks.

Automated User Identity Verification

ID Document Verification and Biometric Verification

AI powered authenticity checks;

Liveness and Likeness to protect against deep fakes and presentation attacks with Signicat VideoID.

eID Hub

World's largest electronic identity hub integrating over 35 eIDs and eID schemes.

Data Enrichment and Verification

Data Verification

The most trusted data sources for checking and validating users' data and for AML screening.

Secure login for returning users

eID Hub

World's largest local eID Hub for identification and authentication with fraud step-ups.

MobileID

Passwordless PSD2 Strong Customer Authentication with geofencing, end-to-end encryption and app-shielding.

Trusted eSignature

AES & QES

Secure signing via Signicat's Electronic Signature API or Signicat Portal and App (Dokobit).

Trust Services

Qualified time stamping, validation, sealing, preserving, storage and archiving of evidence.

Digital Evidence Management

Transaction, signature and consent evidence for audit trails.

Ongoing Identity Monitoring

Continuous verification of customer data updates and compliance both for users and businesses.

Automated user identity verification

Humans are less likely to detect evolving deepfakes, whether in videos, voices or fake ID documents. Innovative **video identity solutions** with powerful AI models will be key in detecting deepfake and synthetic identities. Such products will be able to block injection and presentation attacks.

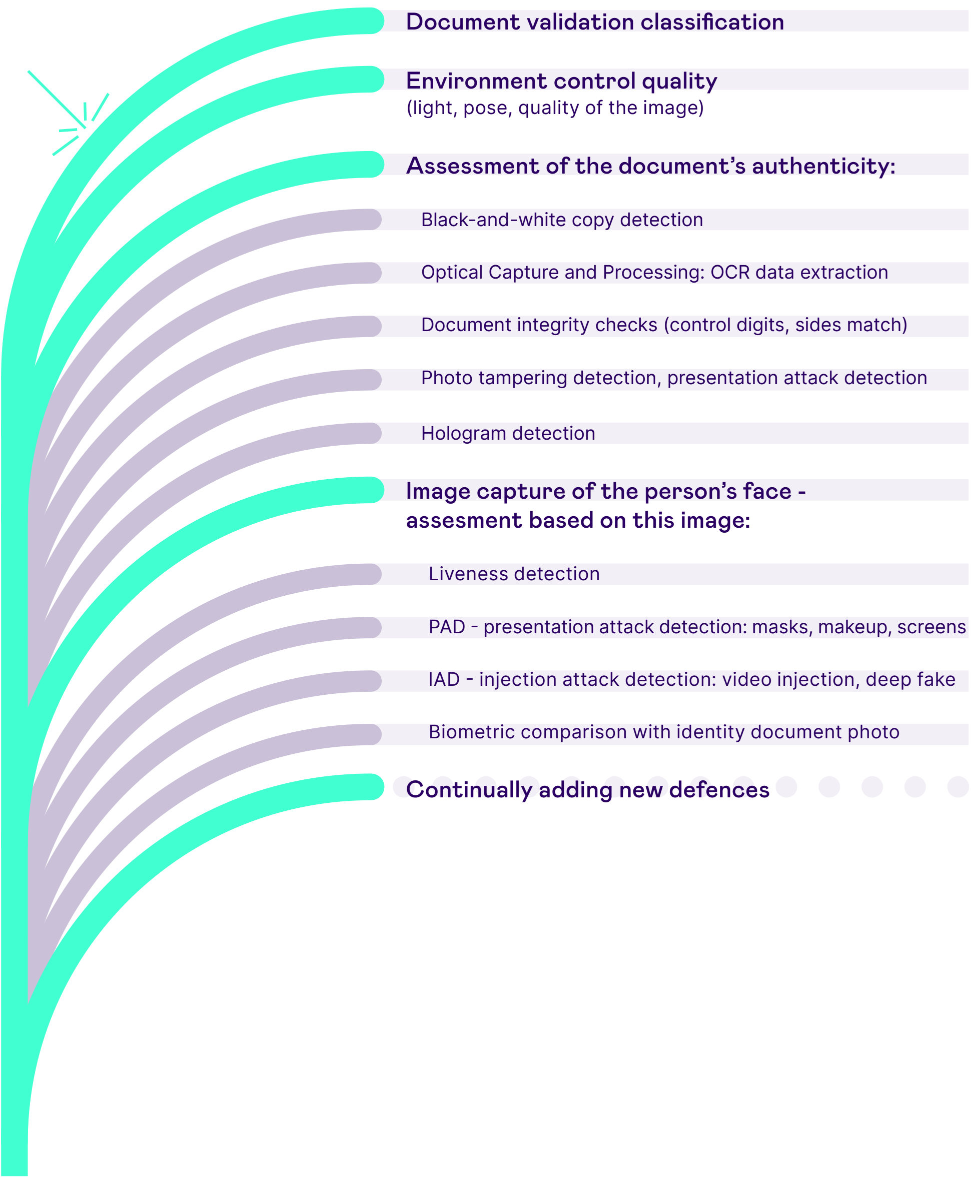
Signicat's VideoID is a certified technology that combines streaming video with artificial intelligence to identify people in real time, within seconds, from any device and through any channel. It has the same level of security and legal compliance as face-to-face identification.*

Remote video identification with VideoID performs automated ID document validation, liveness and likeness checks. Signicat VideoID complies with LINCE standards which cover, among others, biometric attacks (both presentation and injection attacks) as well as an extensive suite of document tampering tests.

Signicat VideoID is a global solution that can be used in more than 150 countries and for more than 530 ID documents.

An agent verification is required for VideoID High.

VideoID: Security built upon AI/Machine learning algorithms



Document validation classification

Environment control quality
(light, pose, quality of the image)

Assessment of the document's authenticity:

- Black-and-white copy detection
- Optical Capture and Processing: OCR data extraction
- Document integrity checks (control digits, sides match)
- Photo tampering detection, presentation attack detection
- Hologram detection

Image capture of the person's face - assesment based on this image:

- Liveness detection
- PAD - presentation attack detection: masks, makeup, screens
- IAD - injection attack detection: video injection, deep fake
- Biometric comparison with identity document photo

Continually adding new defences

eIDs (Electronic Identities) are also a performing shield shield against fraud when onboarding or logging in users. They provide a higher level of assurance about a person, key identity attributes, and user data that can be further verified to prevent account takeover fraud or synthetic identity fraud.

Signicat's eID Hub is the world's largest electronic identity hub integrating over 35 identities and enabling millions of users across Europe to access identity services in a secure, convenient, and efficient way.

Data enrichment and verification for thorough KYC and KYB

Data verification is necessary for KYC and KYB compliance as well as an anti-fraud measure. Data checks can be performed using reliable 3rd party registries.

Signicat Data Verification allows for the retrieval and cross-referencing of customer data for both natural persons and organisations against more than 200 unique service integrations.

Tailored user onboarding flows

"No size fits all" also holds true for KYC, KYB, and onboarding. Orchestration capabilities that support different user segments, risk profiles, markets, regulations, and user types, along with their associated risk profiles, are invaluable for optimising the cost of fraud detection and prevention.

Early checks such as velocity checks, device profiling, and behavioural analytics should be orchestrated in the onboarding workflow. National and local regulations, availability of eIDs, and the level of assurance required, all dictate the need for an optimised automated workflow capable of connecting the different data sources, consolidating identity data and associated risk score.

RiskFlow Orchestration enables creation of tailored and optimised KYC, KYB and AML compliant workflows. It also allows for integration of over 200 data sources in addition to all eIDs from the eID Hub, and Data Verification. RiskFlow Orchestration has the capability to integrate velocity, device and other risk checks to minimise fraud risk and cost.

InstantFlows offer out-of-the-box compliant KYC and KYB workflows, and Signicat Mint is a no-code builder for compliant end-user journeys with a straightforward drag-and-drop interface.

Secure login for returning users

Once users are onboarded, it is key to minimise account takeover fraud by putting in place secure login options. These options can be **eIDs and eID fraud step-ups**, and **biometrics and SCA**, specifically biometrics on mobile devices.

> Signicat MobileID is a PSD2-compliant SCA mobile authentication product using device biometrics
>
> - End-to-end encryption of the communication channel between your SDK and MobileID to prevent man-in-the-middle (MITM) attacks
> - Authentication step-ups for risky transactions leveraging Server Side Biometrics
> - Geolocation and Geofencing
> - Runtime Application Self Protection: extra layer of protection and detection of fraudulent activities

Ongoing identity monitoring

As identity fraud can occur even after users have been onboarded, continuous identity monitoring is key to maintaining the accuracy and compliance of user's information, and the detection of any suspicious activity.

Identity monitoring can include regular cross-checks of user identity information with public and national registries, PEP and sanction lists when required, as well as transaction monitoring (authentications, payment and other financial transactions).

> Signicat Ongoing Monitoring allows for continuous customer due diligence by regularly monitoring customer data against prominent national and commercial registries. This approach ensures safety of your customer relationships. Signicat Ongoing Monitoring can be combined with other Signicat products.

Relying on a team of experts with extensive experience in the European identity space

Regulations and technology are subject to rapid changes, particularly when they differ between countries. Relying on a group of global Digital Identity experts who can design tailor-made solutions in any country is the most efficient way to manage risks and have a single point of access and contact.

Get in touch with a Signicat expert

Signicat

Contact Consult Hyperion

consult hyperion
securing tomorrow's transactions

Methodology

For this report, Signicat engaged independent research house Censuswide to survey 1206 fraud decision-makers across Belgium, Germany, the Netherlands, Norway, Spain, Sweden, and the UK. Survey respondents were drawn from banks, insurance providers, payment providers and fintech, and all were involved in the decision making process in regards to fraud. Answers were collected via an online survey between 22nd March and the 23rd April 2024.

Glossary of terms

Account takeover: A type of identity theft and fraudulent activity where a malicious third-party gains unauthorised access to a user's account credentials, often resulting in misuse or manipulation of the account.

AI-driven identity fraud: The use of AI to support or conduct identity fraud, such as the creation of false documents or the theft of another identity, including for impersonation, document forgery, phishing, and social engineering.

Authorised push payment (APP) fraud: When the legitimate account holder is tricked into making a payment to a fraudster.

Card payment fraud: Any unauthorised use of a payment card or the information associated with it to conduct a fraudulent transaction.

Deepfakes: Videos and voices created using sophisticated software to impersonate real people for scams, fraud, or identity theft.

EBA: European Banking Authority, a regulatory agency of the European Union.

Electronic identification (eID): A digital representation of an individual's or entity's identity, providing secure and efficient ways to prove identities online and access a wide range of services. The authorisation and issuance of eID's are managed by various organisations known as Identity Providers (IdPs). These can include government agencies, private companies and financial institutions.

eID / digital identity fraud: A type of fraud that subverts national digital identity schemes such as Bank ID in Norway or iDIN in the Netherlands, either by taking over an existing account or creating a false identity.

ID document forgery: The practice of creating, copying, and/or altering identity documents, such as identity cards or passports, with the intent to deceive others about the identity or legal status of the holder.

Identity fraud: Encompasses various forms of illegal activities involving personal information. It includes the illegal use of another person's personal information by an individual for criminal purposes, such as ID document forgery, synthetic ID fraud, account takeover, impersonation, and the creation of deepfakes.

Identity theft: The fraudulent use of someone else's personal information, such as their name and financial details, to obtain credit, loans, or other benefits. It involves deceiving victims to obtain sensitive information, which is then misused for unauthorised financial transactions.

Injection attack: Occurs when malware or untrusted input is deliberately inserted into a program, compromising its integrity or functionality. This could involve the insertion of deepfakes or manipulated/untrusted pre-recorded videos.

Malware: Software designed to disrupt, damage, or gain unauthorised access to a computer system.

Man-in-The-Middle Attack (pharming attack): A type of attack in which fraudsters intercept communication between two parties and steal data or redirect users to a malicious website.

Occlusion attack: Occurs when fraudsters conceal part of their face to bypass video controls, often used to deceive liveness challenges.

Phishing: The fraudulent practice of sending emails or messages purporting to be from reputable companies to induce individuals to reveal personal information.

Presentation attack: Involves fraudsters using spoofs to impersonate someone else, such as using masks, makeup, or displaying a face on a screen.

PSD3: The third Payment Services Directive, enhancing the security and efficiency of digital payments and financial services in the EU, promoting innovation and competitiveness in the financial sector.

Synthetic ID fraud: Involves stealing a genuine person's information and combining it with fabricated personal data to create a false new identity.

Signicat

The Battle Against AI-driven Identity Fraud

2024