# Identity Fraud Report

# Contents

# Introduction

"We are pleased to publish the first edition of our identity fraud report, which explores the fraud trends we've seen over the past 24 months. We delve into why we believe a layered approach to fraud detection provides the best results - using a combination of technology and a team of verification experts to keep businesses and people safe.

As an identity provider, we have a unique insight into the techniques fraudsters are using. We can see where they are focusing their efforts and how these are changing over time. We continue to develop our tools to ensure we stay at the forefront of detecting and preventing fraud."

***Mick Larkin***
*Global Operations Manager and Fraud Expert at Yoti*

***Mykola Voloshyn***
*Fraud Team Lead at Yoti*

**All data in this report is taken from our Security Centre.**

# Fraud landscape

## Businesses have got better at detecting fraud

Fraud stats are on the increase. There are many headlines and scaremongering stories about the rise in fraud.

But in reality, nobody really knows whether fraud itself is increasing or decreasing. Businesses are only able to report on the fraud they do know about. Most fraud figures are only estimates; it's challenging to understand the exact figures and the true scale of fraud.

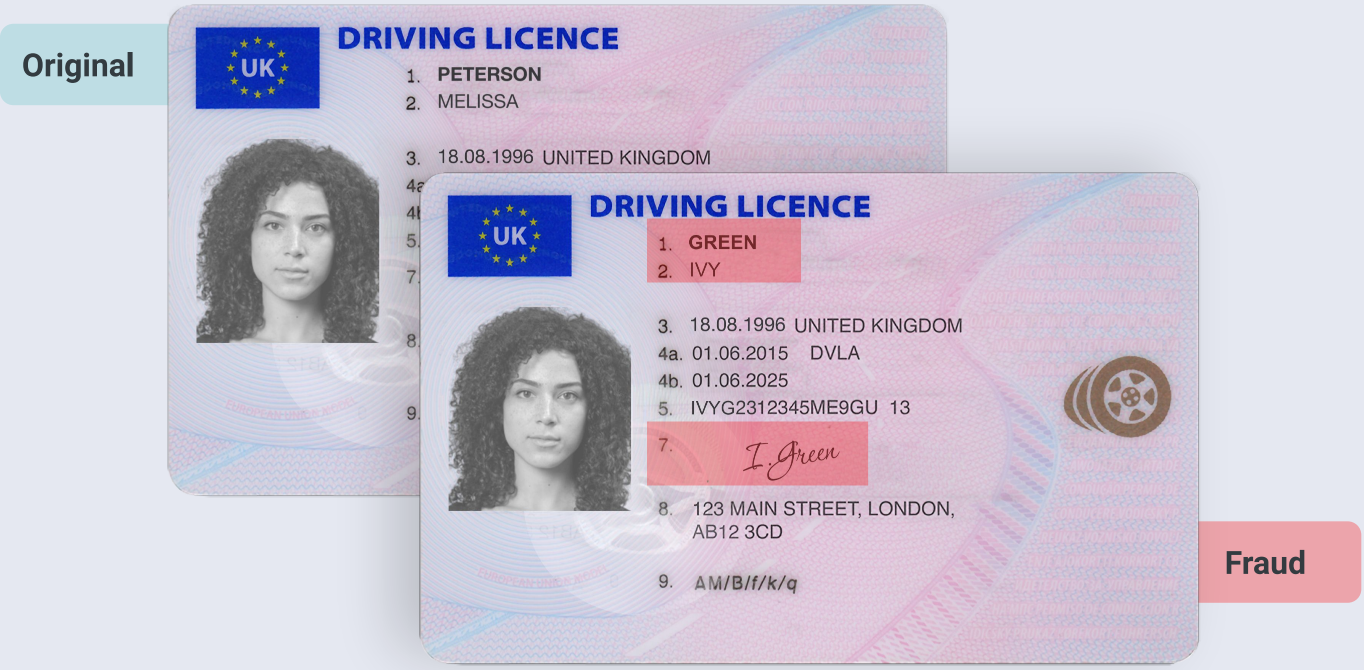
One reason why fraud numbers continue to rise is because businesses have got better at detecting fraud. If a business can detect more fraud, they have more numbers to report on. Businesses are able to identify attempted fraud thanks to advances in technology:

- Fraud monitoring tools and software can detect suspicious activity or transactions
- AI and automated technology can detect fraudulent identity documents
- Better links with external and third party databases

## Fraud is becoming accessible to more people

As the world becomes more digitised, we are seeing significant variations in the quality and types of fraud. A lower level of fraud (fraud which can be achieved for minimal effort) is becoming accessible to more people.

This is because the equipment needed to produce fraudulent documents is becoming cheaper. It's also easier to obtain fake versions of certain document types, such as driving licences and national IDs, and templates to create fake documents are easily accessible to anyone online. Fraudsters are taking advantage of this 'low hanging fruit' - looking for areas which are easy to exploit for minimal effort.


Original
Fraud

UK DRIVING LICENCE
1. PETERSON
2. MELISSA
3. 18.08.1996 UNITED KINGDOM

UK DRIVING LICENCE
1. GREEN
2. IVY
3. 18.08.1996 UNITED KINGDOM
4a. 01.06.2015 DVLA
4b. 01.06.2025
5. IVYG2312345ME9GU 13
7. I.Green
8. 123 MAIN STREET, LONDON, AB12 3CD
9. AM/B/f/k/q

## Fraud is evolving

Businesses have to deal with and be prepared for different types of fraud. Fraudsters are constantly evolving and using different tactics and approaches, including deepfakes, fake documents, impersonation attempts and account takeovers. The quality of fake IDs (generated by AI) is now incredibly sophisticated, with fraudsters churning out masses of digital fakes in minutes. As fraudsters continue to innovate and evolve, the technology and tools to detect and prevent fraud also needs to adapt.

# Fraud trends

Over the past 12 months our Security Centre has seen an increase in the number of impersonation attempts and a rise in counterfeit documents.

## Impersonation attempts

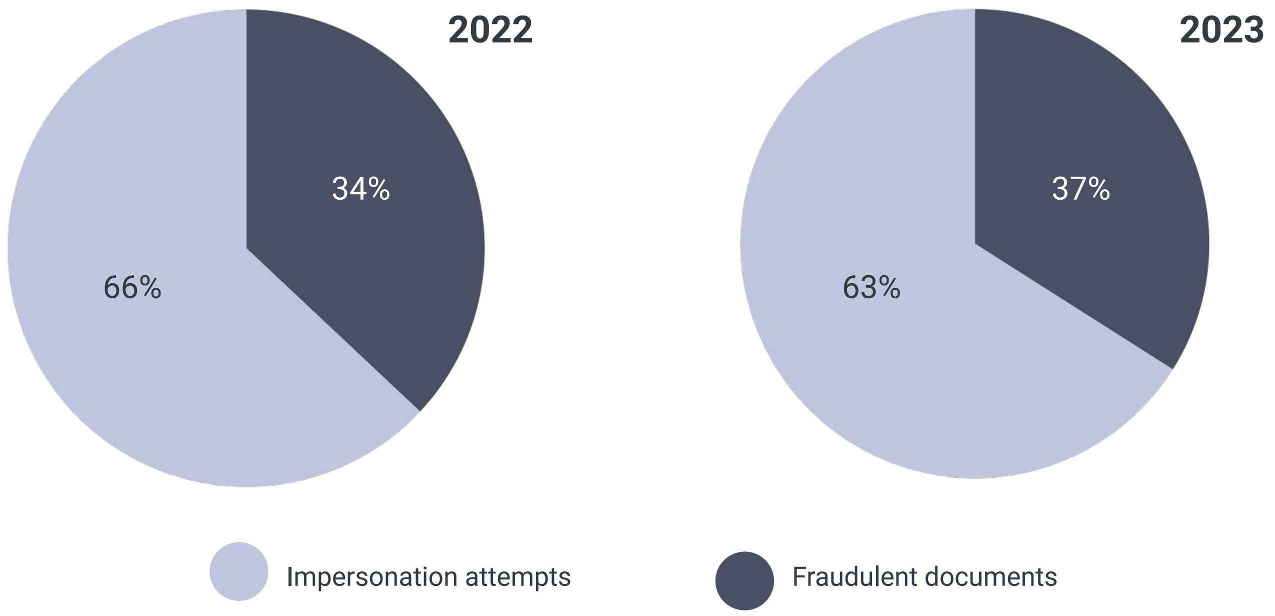
Impersonation attempts now makeup two-thirds of the fraud we see. This is when the selfie a user submits doesn't match the photo on the identity document.

Impersonation attempts could happen for several reasons. Not all are fraud-related:

- Someone is attempting to use another person's document (fraud)
- They have not understood the instructions
- The selfie is poor quality so we can't clearly match the image on the identity document to the selfie
- They might have changed their appearance drastically since the ID photo was taken - making it challenging to match the photos

In 2022, our Security Centre saw more impersonation attempts, where the face on the identity document does not match the selfie. But in 2023, we started to see an increase in the number of fraudulent documents being used:

### Fraud activity, as recorded by the Security Centre:



# Fraudulent documents

Fraudulent documents can fall into the following categories:

- **Tampered with**
  An altered version of an original document.
- **Counterfeit**
  A reproduction of an original document. A false document which imitates something genuine.
- **Compromised**
  Genuine documents that have been found online. Anyone can take a screenshot or picture of them.
- **Sample**
  Publicly available sample document templates.
- **Fantasy or Camouflage**
  Also known as 'fantasy' or 'pseudo' documents, these are not real documents. They may be issued in the name of an existing place, or a non-existent country or state. The 'type' of document is complete fiction.
- **Fraudulently obtained genuine (FOGs)**
  Genuine documents which are obtained and misused by a fraudster. They are obtained by submission of either false or counterfeit documents, cooperation of a corrupt official or impersonation of the rightful holder of a genuine document.

## Document fraud typically falls into four levels of sophistication:

**Level 1:** These are very basic attempts at committing document fraud and can usually be identified quickly and easily.

**Level 2:** These are poorly manufactured or altered document templates. They're slightly more sophisticated than the amateur documents in level 1. They can typically be detected by looking at number formats, data inconsistencies, and security features being missing or inconsistent.

**Level 3:** These are sophisticated document forgeries and counterfeits. All of the data present on a level 3 document is correct and makes logical sense, but trained experts and ad-hoc tech can detect small variations in fonts, layout, and security features.

**Level 4:** The most sophisticated attempts at ID fraud. These can only be spotted thanks to expert third parties such as CIFAS and Amberhill as these mostly fall in the Fraudulently Obtained Genuine (FOGs) category. These are genuine, real documents, so expert third parties are needed to confirm if the documents are fraudulent or not.

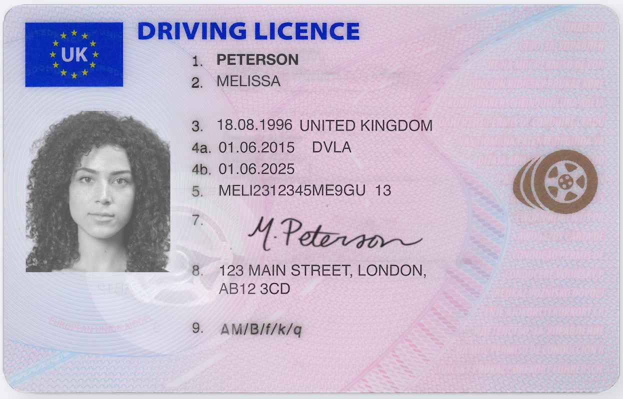
**Each level of sophistication comes with a different cost and time. We have provided approximations for these below:**

| Level | Level 1<br>(Low Quality) | Level 2<br>(Medium Quality) | Level 3<br>(High Quality) | Level 4<br>(Highest Quality) |
|---|---|---|---|---|
| Time taken | 5 to 30 minutes | Up to 1 hour | Up to 4 hours | Over 4 hours |
| Cost in £ | £0 - £50 | £50 - £100 | £100 - £1000 | £1000+ |

## The different categories of fraudulent documents can fit into more than one level:

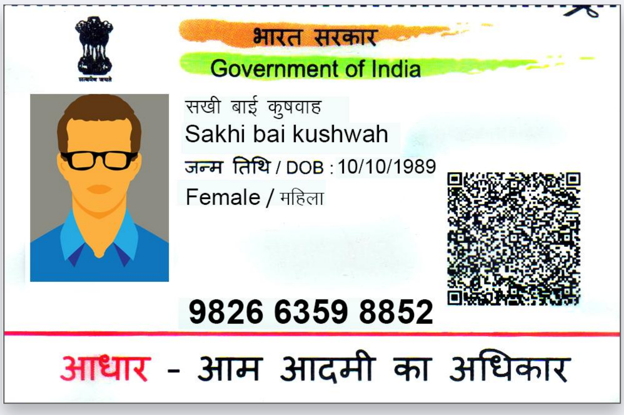
The vast majority of fraudulent documents that come through to our Security Centre are tampered with or counterfeit. It is worth noting that a substantial number of the documents we class as fraudulent are specimen documents when clients are testing the technology.

**Over 50% of the document fraud that comes through to our Security Centre relates to Driving Licences and National IDs**



UK DRIVING LICENCE

1. PETERSON
2. MELISSA
3. 18.08.1996 UNITED KINGDOM
4a. 01.06.2015 DVLA
4b. 01.06.2025
5. MELI2312345ME9GU 13
7. M.Peterson
8. 123 MAIN STREET, LONDON, AB12 3CD
9. AM/B/f/k/q



भारत सरकार
Government of India
सखी बाई कुषवाह
Sakhi bai kushwah
जन्म तिथि / DOB : 10/10/1989
Female / महिला
9826 6359 8852
आधार - आम आदमी का अधिकार

Over the past two years, we've see the highest percentage of **fraudulent driving licences** from Sri Lanka, Thailand, Portugal, Lithuania and Nigeria.

We've seen the highest percentage of **fraudulent national IDs** from Cyprus, Poland, Indonesia and Slovenia.

Our automated technology and team of verification experts can identify fraudulent documents from over 200 countries and territories. This helps to keep your business safe from fraudulent attempts, no matter where you operate.

To test our systems and, with consent, those of any suppliers we are evaluating, we also create and purchase fake identity documents of varying quality, and tamper with images of legitimate documents.

If you'd like to find out more information about the fraudulent documents we identify, please get in touch.

| Level | L1<br>(Low Quality) | L2<br>(Medium Quality) | L3<br>(High Quality) | L4<br>(Highest Quality) |
|---|---|---|---|---|
| Counterfeit | 🟢 | 🟢 | 🟢 | 🔴 |
| Tampered | 🟢 | 🟢 | 🟢 | 🔴 |
| Compromised/Sample | 🟢 | 🟢 | 🟢 | 🔴 |
| Fantasy/Camouflage | 🟢 | 🔴 | 🔴 | 🔴 |
| FOGs | 🔴 | 🔴 | 🔴 | 🟢 |

# The market for fraudulent documents

There is a better utility and market for fraudulent documents. Fraudsters are continually looking at ways they can circumvent identity checks or create better fake documents.

## Creating fake documents

Technology developments assist in the creation of fraudulent documents. For little effort and low cost, someone could create a fake document image in minutes. Certain sites even allow people to purchase security features like holograms that are a replica of the ones used on genuine documents. For instance, they can buy 1,000 holograms for less than £200.

Additionally, the quality of fake digital IDs, generated by AI, is now incredibly sophisticated, and easily available. OnlyFake, an underground website claiming to use "neural networks", can create highly convincing synthetic IDs using AI for just $15.

## Tampering with genuine documents

It is easier to tamper with a document than try to create a fake one from scratch. This is reflected in our own data; since July 2023 we have started seeing more tampered with documents compared to completely fake ones.

## Exploiting weaknesses in verification processes

Fraudsters may also exploit weaknesses, such as when a physical document is not required for a verification process, but a scan or image of a document can be used instead. In such instances, a Photoshop subscription costing around £20 a month, or a pirated version coupled with some basic design skills would be enough to pass some verification requirements.

It is very easy for someone to buy the equipment to make fake documents or tamper with real ones, and some documents are very easy to replicate. There's a whole list of reasons why some people attempt to create and use fraudulent documents:

- To sell to underage people who want to get into a nightclub or buy age-restricted items
- To sell to people who do not want to use their real identity to complete a transaction or verification process
- To open bank accounts or apply for credit in another person's name

# Yoti’s approach to fraud detection

Any business that interacts with customers needs to know if the customer is ‘good’ and providing genuine details, or if they are a ‘bad’ fraudulent customer. There is no one-size-fits-all when it comes to mitigating fraud. That’s why we offer a layered approach to fraud detection.

We offer our automated process as a minimum level for all businesses. For companies, especially those in highly regulated sectors or those who have a lower appetite for risk, they can then layer on the skills of our verification experts.

It is imperative that regulators regularly review the minimum requirements for customer due diligence and authentication in regulated sectors. They should state which elements of fraud detection are a minimum acceptable level, looking at layer 1 (automated processes such as document authenticity checks and liveness technology), and layer 2 (using verification and counter fraud experts).

## Layer 1 - Automated processes

- Document authenticity checks
- Face matching
- Liveness technology
- Secure Image Capture (SICAP)
- Third party databases

## Layer 2 - Verification experts

- Super Recognisers and Face Matchers
- Counter Fraud Team

# Layer 1 - Automated processes

## Document authenticity checks

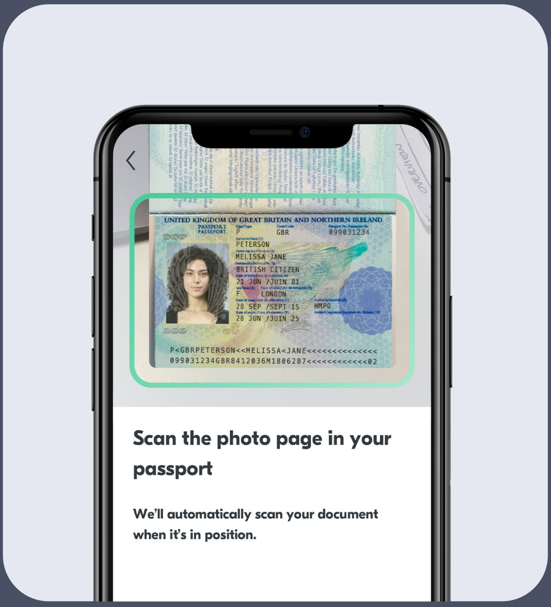
We complete various document authenticity checks to determine if the document:

- is a government-issued identity document
- is valid
- is in date
- has been tampered with
- is a counterfeit
- is a known lost or stolen document

Without this step, people could use anything that looks vaguely like an identity document and it could be accepted. It's relatively easy to buy a 'novelty' or fake document, tamper with a sample or genuine document, obtain a document from the dark web, or create a synthetic fraud.

By detecting fraudulent documents early in the customer journey (for example during onboarding), this can prevent more fraud later on.

### How document authenticity checks can combat fraud


UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
PETERSON
MELISSA JANE
BRITISH CITIZEN
P<GBRPETERSON<<MELISSA<JANE<<<<<<<<<<<<<<<<

**Scan the photo page in your passport**

We'll automatically scan your document when it's in position.

### Age Verification

A document authenticity check is used as part of the verification process to give a high level of confidence that the document is real

**Why is this important?** - a stolen, fake or tampered with document could pass an age check

**Example use case** - you need to confirm that everyone who signs up to your online platform is 18+. Users can use an identity document to prove their age. Document authenticity checks prevent minors from using a fake document.

## Face matching

Face matching is a very important step in an age or identity verification process. It assesses if the person presenting the document matches the photo of the person on the document. Without this step, someone could use another person's document.

## Liveness technology

Liveness is an essential part of any verification or authentication process. It gives you reassurance that you are dealing with a real human.

Liveness does not recognise who the person is (that's facial recognition), and it does not check a face against faces in a database. It is most commonly used in combination with other authentication factors to ensure that authentication or verification isn't being spoofed.

Liveness combats what is technically termed "presentation attacks". Without liveness, you could be susceptible to a presentation attack. These could be:

- Paper images
- Masks
- Screen images
- Video imagery
- Deep fake videos
- Bot attacks

Our proprietary passive liveness technology, MyFace, verifies that a user is a real person, and not a presentation attack such as a printed or digital photo, video or mask – all from a single image.

Passive liveness doesn't require any action from the user and works from a single selfie. Unlike active liveness, users do need to perform any actions or movements to prove their 'liveness'. This creates a better user experience for the 'good' customers, reduces drop off and speeds up the customer journey. It is also simpler for people with accessibility needs - making it a more inclusive solution.

Genuine customers do not object to efficient and effective security layers. In fact most customers appreciate companies taking the time, effort and expense to ensure their assets, accounts or finances are being kept safe.

MyFace can strengthen age and identity checks, prevent account takeovers and protect individuals and businesses against the growing risks of identity fraud.

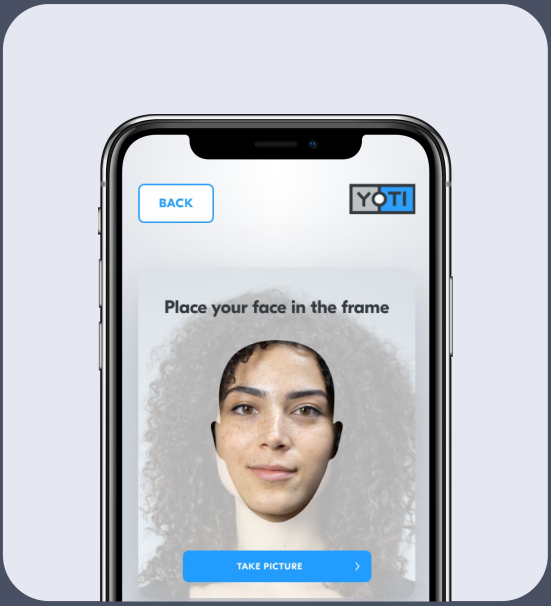
iBeta QUALITY ASSURANCE TESTED
LEVEL 2
ISO 30107-3
Presentation Attack Detection
COMPLIANT

MyFace is compliant with iBeta NIST Level 2. NIST (National Institute of Standards and Technology) provides a framework for testing performance levels of liveness. Since achieving **iBeta Level 1 in February 2022**, we continued to develop our liveness technology.

Level 2 involves training and testing the technology against more expensive, specialist attacks such as 3D printers, resin and latex face masks. To achieve Level 2, the liveness technology must detect 99% of attacks. **Our liveness solution achieved a 100% detection rate.** Level 2 is the maximum level that iBeta and other NIST-accredited labs currently certify against.

Our liveness technology can return a result within three seconds. Combined with our patented SICAP (**S**ecure **I**mage **Cap**ture) solution, this is a significant barrier to spoofing, Generative AI and deepfake attacks.

## How liveness technology can combat fraud



### Identity Verification

Liveness is used as part of the verification process to give a high level of confidence that the check is real

**Why is this important?** - a stolen document plus a fake image could spoof an identity check

**Example use case** - your customer wants to open a new bank account and needs to prove their identity. Liveness ensures the person signing up is a real person. Liveness is used in combination with data extraction, document authenticity and face match for a secure verification process.

## Secure Image Capture (SICAP)

Injection attacks are a growing threat to online verification processes, as fraudsters attempt to bypass liveness detection by injecting manipulated images, videos, or even artificially generated content to spoof authentication systems. SICAP prevents fraudsters from bypassing the device camera to 'inject' an alternative image or video.

SICAP, short for **S**ecure **I**mage **Cap**ture, is a proprietary technology, part of which is patented, that works alongside Yoti's liveness detection capabilities. SICAP can identify and prevent more sophisticated injection attacks, ensuring that the images captured during a verification process are genuine and remain untampered with.

> "As the threat of generative AI in identity verification accelerates, we have developed a comprehensive strategy focused on early detection. We are committed to developing leading technology which is at the forefront of combating evolving threats in the generative AI landscape. The combination of our liveness technology and SICAP solution gives businesses enhanced security and defence against fraudulent attempts and deepfakes."
>
> **Paco Garcia**
> CTO at Yoti

## Third party databases

We are members of CIFAS, Amberhill and Synectics. By having access to their databases of fraudsters, we are alerted to known fraudulent activity. This could flag a known police operation of an Organised Crime Gang for a fake document factory, or it could be a unique fraudster that has a filed record.

By having a reciprocal relationship with these companies and their members, this allows all parties to reduce overall fraud.

# Layer 2 - Verification experts

Another line of defence to help detect and prevent fraud is our team of verification experts. For the trickier submissions or when technology can't provide a high level of confidence, our 150-strong team of Super Recognisers, Fraud Experts and Face Matchers are here to help.

## Super Recognisers and Face Matchers

Our Super Recognisers and Face Matchers provide an extra layer of security and really come into play here – combing through images and documents to look for fake aspects and to provide a necessary human check. They are not there to replace technology, but to work alongside it. The highly skilled abilities of our Super Recognisers can sometimes provide clarity where technology may struggle. Most of our human fallback capabilities are processed in under 90 seconds.

**Human fallback is particularly valuable when:**

People fail the automated solution. This could be for a number of reasons, including:

- The user has not understood the instructions correctly
- Poor lighting means the technology might struggle to read the identity document
- The photo on the user's identity document might be over 10 years old. If the user's appearance has changed a lot since the photo was taken, automated technology might struggle to match the images
- Poor quality or damaged documents can be difficult for technology to read

All of these instances will need to be picked up by a human fallback team. This could be upwards of 30% of verifications.

Additionally, automated solutions do not spot as much fraud as a team of experts. For instance, it can sometimes be difficult for automated technology to recognise all of the various security features across hundreds of documents from around the world. Our security team can do a detailed inspection of the features on a document to check its authenticity.

> “Automation plus humans gives businesses extra confidence and peace of mind that the verification process is robust, effective and accurate. Crucially, it also ensures higher completion rates, improves onboarding rates without additional friction and reduces identity verification costs. This is especially important for highly regulated sectors where it’s critically important to get it right. As such, they can request our human fallback for added security and confidence.”
>
> **Louise Bruder**
> Security Centre Training Manager and Super Recogniser at Yoti

Our team is also trained to spot morphed images. A morphed photo is the process of taking images of two different people and blending them together until they form a ‘third’ person. This final image takes on attributes of the two original identities, making it harder to determine if the image is fake. This can be particularly challenging when the two original identities share similar features to begin with.

There are many reasons why someone may create a morphed image, but one type of fraud where this is more prevalent is to obtain a fraudulently obtained genuine document (FOGs). Modern passports contain counterfeit prevention measures (for example, patterns visible only under specific light) which make any attempts to alter or duplicate the document itself easier to detect.

Fraudulently obtained but genuine passports are real documents which are wrongly issued to fraudulent applicants. They arise when a fraudster has a genuine passport and submits a renewal application using a morphed photo of a similar looking person. If this morphed photo goes undetected and is incorrectly matched to the original passport image, a fraudulently obtained genuine passport is issued to the fraudster. They can then use this to travel, obtain other fraudulent identity documents, or open bank accounts under a false identity.

We have invested time and effort building a service that records various attack vectors and fraudulent activity. An intrinsic part of our manual fallback service is keeping a record of fraudulent documents and faces. This allows us to help our clients detect and prevent fraud - especially from repeat offenders.

## Counter Fraud Team

We also have a dedicated Counter Fraud Team, who hold professional certificates in Fraud Prevention. They not only analyse any fraud submissions we receive but also complete robust research into fraud trends globally. This helps them to stay at the top of their game to spot fraudulent documents.

Our Security Centre operates 24/7, working around the clock to keep your business safe from fraud.

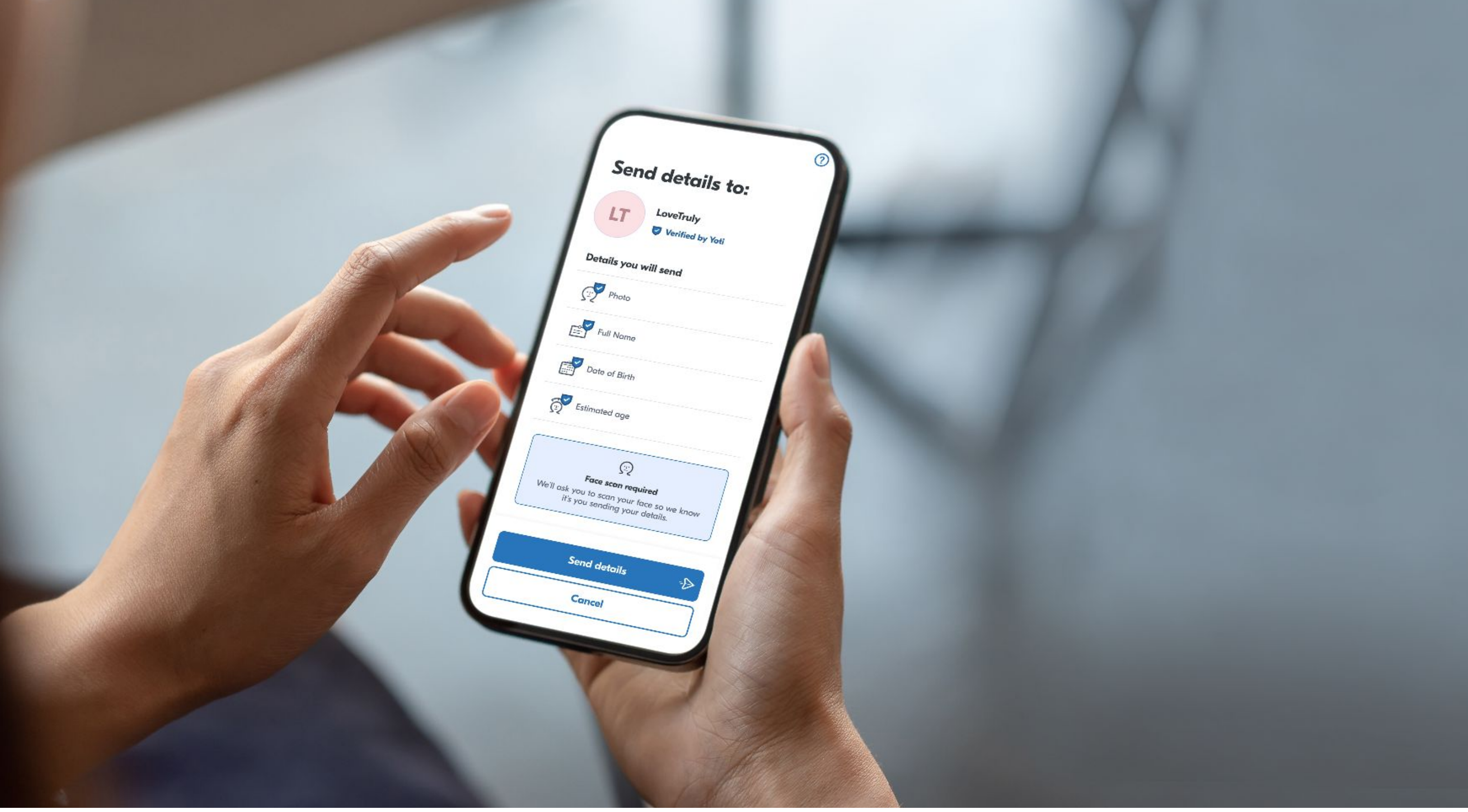
# Making identity checks safer with Digital IDs

A Digital ID gives people a safer and instant way to prove their age and identity from their phone, with no need to show identity documents or share an unnecessary amount of personal data.

Digital IDs allow businesses to identify and authenticate customers to the highest standards. Whether online or in person, you can be confident you know who you're dealing with, strengthen security, enhance privacy and improve the customer experience.

When someone first creates their Digital ID, we verify their identity to a government-issued document. This gives businesses confidence that the details someone shares from their Digital ID are genuine and correct.

Digital IDs provide a strong line of defence against fraudsters providing fake details or attempting to use another person's documents to complete a verification check.



## Data minimisation

Our Digital IDs apps (Yoti ID, Post Office EasyID and Lloyds Bank Smart ID) allow people to share specific information. So if they only need to prove their age, they can share their date of birth or even ‘over 18’, without sharing any other details.

This is a safer approach to relying on identity documents to confirm a customer’s age or identity. After all, it’s not possible to use an identity document as proof of age or address, without sharing all of the details on that document. This results in people sharing more information than necessary, putting them at greater risk of identity theft.

## Valuable documents can be kept safe at home

A Digital ID eliminates the need to carry around and use physical identity documents, which can be easily lost, damaged or stolen. This is mainly a problem for young people who need to show physical ID more frequently than those who look visibly older.

By using a Digital ID as proof of age or identity, valuable documents like passports and driving licences can be kept safe at home.

Losing a passport is not only an inconvenience and costly to replace, but it can leave people extremely vulnerable to identity theft and fraud. If a passport falls into the wrong hands, that person could use the document to open bank accounts, apply for credit, and create fake social media accounts – all in the owner’s name.

## Peer to peer identity checks

A unique feature of our Digital ID app is the ability for users to share verified information with other people.

With more people connecting online to find tradespeople, for online dating or to exchange items on marketplaces, this has also led to a rise in online scams. With the Yoti ID and Post Office EasyID apps, users can swap verified details with other people, for free. It gives them a quick, secure and simple way to know who they're really connecting with.

## Privacy-preserving

From the way we build our products, our security certifications and audits, our unique approach to data storage and our ethical principles – we are committed to upholding the highest security standards throughout every part of our business.

Our seven ethical principles guide our everyday decisions and ensure that we always strive to do the right thing. They have a strong focus on how we enable privacy and anonymity, how we keep sensitive data secure, and how we're transparent and held accountable

## More transparency and control over personal information

By sharing data piece by piece, people know exactly what they are sharing with a business or another person. They have a record of this in their Digital ID app and always consent to share their data. Digital IDs also reduce the need for individuals to complete lengthy forms or scan and upload documents.

## Stronger security

We've built our Digital ID app with privacy and security at its core. It has been carefully designed to put users in control and to protect their privacy and personal data at all times.

Each piece of data is encrypted, made unreadable and then stored in its own individual safe – which only the user can access on their phone. Should their phone fall into the wrong hands, their Digital ID is protected by a PIN that only the user should know, and linked to their personal biometrics for added security.

Our database is protected by high-level security. We also follow the highest standards of security. We're certified to meet SOC 2 Type II and ISO/IEC 27001, the global gold standard for information security management.

# Final thoughts

With more services moving online, the importance of fraud detection and prevention has never been more important. Key trends we've highlighted in our first identity fraud report include:

## Businesses have got better at detecting fraud

Whilst it's difficult to say with absolute certainty whether or not fraud is increasing, what we do know is that businesses are detecting more fraud. It remains a challenge to know exact figures and the true scale of fraud; businesses can only report on the fraud they do know about and much goes undetected or unreported.

## Fraud is becoming accessible to more people

As the world becomes more digitised, we are seeing significant variations in the quality and types of fraud. Some fraudsters are looking for quick wins and low hanging fruit - capitalising on weaker security systems. Others are using more sophisticated techniques, utilising advances in AI to commit a higher level of fraud. The quality of fake IDs, deepfakes and synectic fraud, generated by AI, are now incredibly sophisticated, with fraudsters churning out masses of digital fakes in minutes. As fraudsters continue to innovate and evolve, the technology and tools to detect and prevent fraud also needs to adapt.

## Fraud is evolving

Businesses have to deal with and be prepared for different types of fraud. Fraudsters are constantly evolving and using different tactics and approaches, including deepfakes, fake documents, impersonation attempts and account takeovers.

As fraudsters continue to innovate and evolve, we continue to develop our tools to ensure we stay at the forefront of detecting and preventing fraud. With a combination of leading AI technology and a highly skilled team of verification and fraud experts, we can help businesses and people to stay safe in an increasingly digital world.

To find out how we can protect your business from fraud, please contact us at **www.yoti.com/contact/business/**