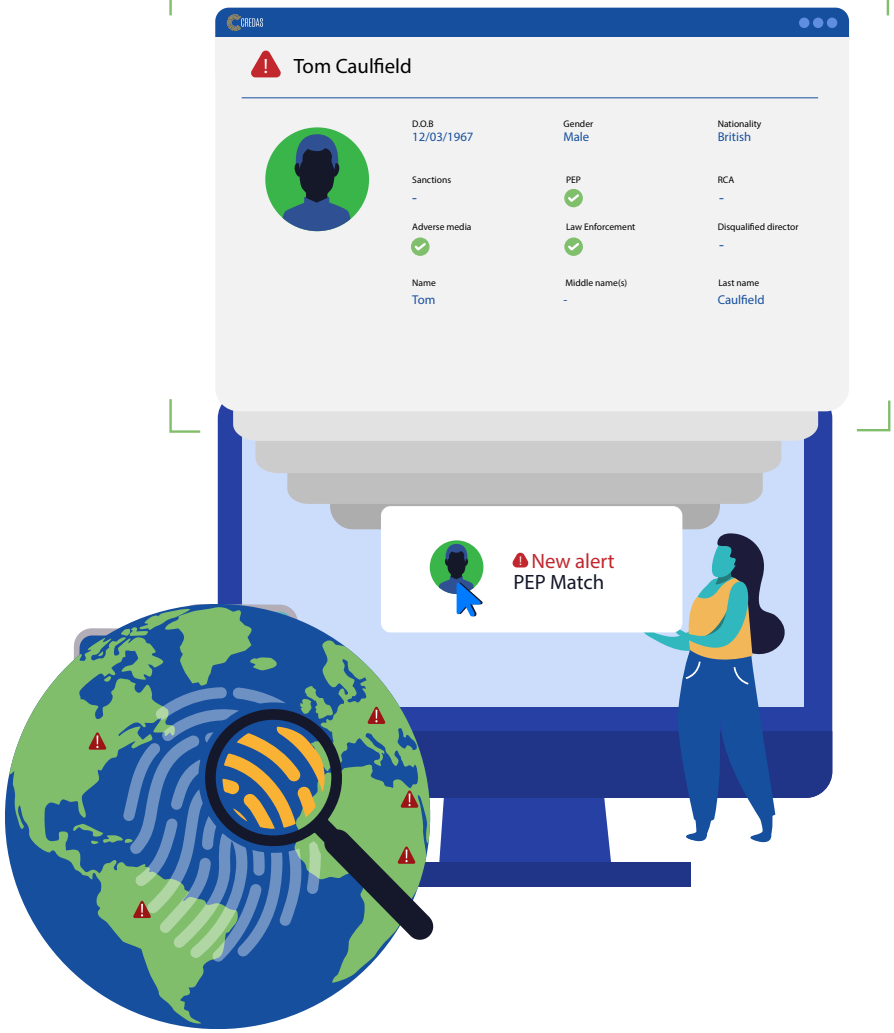
CREDAS
A Dye & Durham Solution

THE CREDAS GUIDE TO COMPLIANT ID CHECKS

THE CREDAS GUIDE TO COMPLIANT ID CHECKS

Contents

Appendices



WHY YOU NEED TO VERIFY SOMEONE'S IDENTITY

Over the last decade, how we shop, work, and live has dramatically changed. Advancements in technology have meant we interact more online, through emails, through the phone, and less in person.

These technological advancements have helped speed up tedious and drawn-out tasks. A few taps on a phone have replaced the need to walk into your bank to get a statement. While these changes have brought many benefits, they have also introduced new risks and opportunities for criminals to exploit.

Criminals have always created false or synthetic identities as a means of concealment, allowing them to operate with a reduced risk of being caught. They also co-opt other people's identities to defraud them of their assets, such as property fraud, or to place the blame elsewhere.

While many people would think the police are solely responsible for stopping and preventing these criminal acts, UK money laundering regulations and immigration law impose some of this responsibility on regulated firms.

It is not good enough for UK businesses to plead ignorance, so regulated firms must understand the laws that apply to them and take the necessary steps to prevent illegal work, property fraud, and money laundering. Those necessary steps include having processes in place to check and confirm their clients' identities.

If you're asking yourself, 'But how?' then you've downloaded the right document. Over the next few pages, we will explain how you can compliantly verify someone's identity, how modern technology can help, and best practices to help keep your business compliant.

To begin with, we will explain the difference between claimed and confirmed identities and the varying degrees of confidence you can have in someone's identity as set out by the Government's Good Practice Guide (GPG) 45.

Knowing Your Customer shouldn't be a game of Guess Who

CLAIMED V CONFIRMED IDENTITIES

Imagine you're an accountant. A client contacts you to manage their financial transactions, including transferring funds from the sale of one business to investing in another.

Much of your communication with the client occurs remotely, primarily over the phone or through email, as they are occupied with managing their business affairs. In this scenario, how can you be certain that the client is truly who they claim to be?

The need for secure and reliable identity verification is crucial in financial transactions. You need to be certain you know who you are dealing with, but how do you go about doing that?

There are many methods to verify someone's identity; for a long time, these checks were done manually, seeing ID documents in person or obtaining copies. You can check someone's ID by post, by phone, by email, in person or digitally. Each method has its own risks and levels of confidence, so which do you choose?

In 2014, the UK government published Good Practice Guide 45, which outlines the best practices for identity verification for organisations in the public and private sectors to ensure secure and reliable processes.

The guide covers topics such as authentication methods, risk management, and the implementation of identity assurance systems. The guide aims to assist organisations in establishing robust and effective measures to verify the identity of individuals, especially in digital and online contexts. GPG 45 outlines five steps you should take when verifying a customer's identity and connecting the person claiming that identity.

MONEY LAUNDERS

Criminals use fake identities, so should they come under investigation, any assets cannot be connected and therefore can't be used as evidence of their crimes or confiscated.

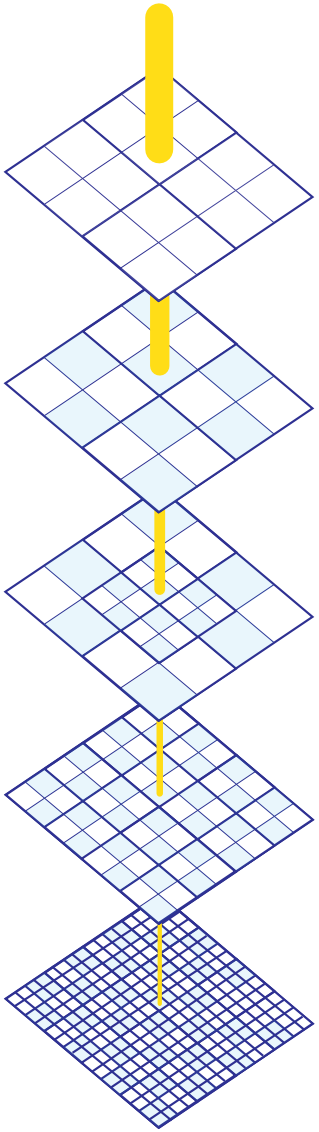
PROPERTY FRAUD

A tenant is attempting to sell their property by claiming to be their landlord. They have access to the property and to letters sent to the property, such as a council tax bill providing evidence to spoof others.

HUMAN TRAFFICKING / MODERN SLAVERY

Human traffickers frequently provide their victims with fake or stolen identities to secure work or rental properties. They also use proxies to pass weak identity checks that don't connect the individual with the claimed identity.

THE 5 STEPS OF IDENTITY VERIFICATION



There are 5 key steps, with each step adding an additional layer of protection that makes it harder for bad actors to get through.

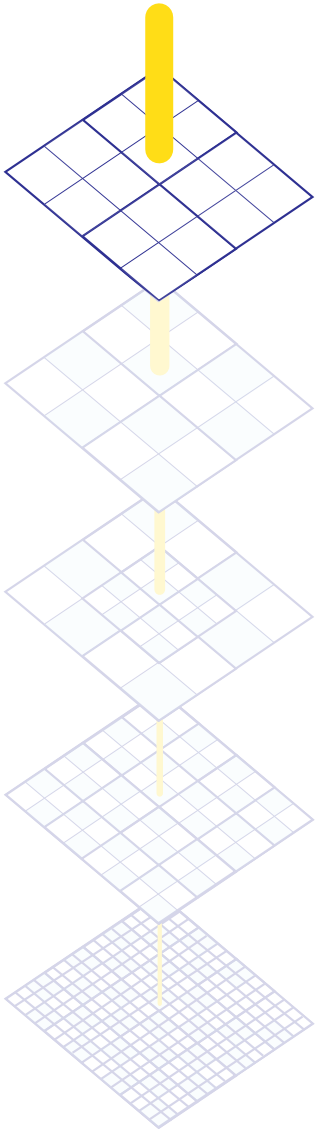
GET EVIDENCE OF THE CLAIMED IDENTITY
Obtain documentation or information that the individual asserts as proof of their identity, such as official identification cards, passports, or relevant personal details.

CHECK THE EVIDENCE IS GENUINE OR VALID
Verify the authenticity and validity of the provided evidence, ensuring that it is not forged or manipulated. This step involves scrutinizing documents for security features and confirming their legitimacy.

CHECK THE CLAIMED IDENTITY HAS EXISTED OVER TIME
Confirm the continuity of the claimed identity over a period, examining historical records or data to establish that the identity has a consistent and legitimate presence over time.

CHECK IF THE CLAIMED IDENTITY IS AT HIGH RISK OF IDENTITY FRAUD
Assess the likelihood that the provided identity is susceptible to fraudulent activities. This involves evaluating factors that may increase the risk of identity theft or misuse.

CHECK THAT THE IDENTITY BELONGS TO THE PERSON CLAIMING IT
This step involves cross-referencing information and additional measures such as biometric recognition and confirming control of submitted documents.



STEP 1 - GET EVIDENCE OF THE CLAIMED IDENTITY

The first step is to collect evidence of the customer's claimed identity. You can do this physically by obtaining the documents or digitally by using an Identity Verification Service Provider (IDSP).

But what is actually considered evidence?
Evidence can range from ID documents like passports or driving licences to copies of utilities/bank statements.

At the most basic level, the evidence should come from a reputable source and contain at least 2 of the following pieces of information.

- the claimed identity's name
- the claimed identity's date of birth
- the claimed identity's place of birth
- the claimed identity's address
- the claimed identity's biometric information (these are measurements of biological or behavioural attributes, like an iris or fingerprint)
- a photo of the claimed identity
- a reference number

Some documents are easier to forge or tamper with, and others are not considered as 'strong'. Forging a driving licence is a lot harder than forging a bank statement. The stronger the evidence, the more confident you can be in the person's claimed identity. Additional security features such as holograms or embedded cryptography will also make verifying these documents much easier.

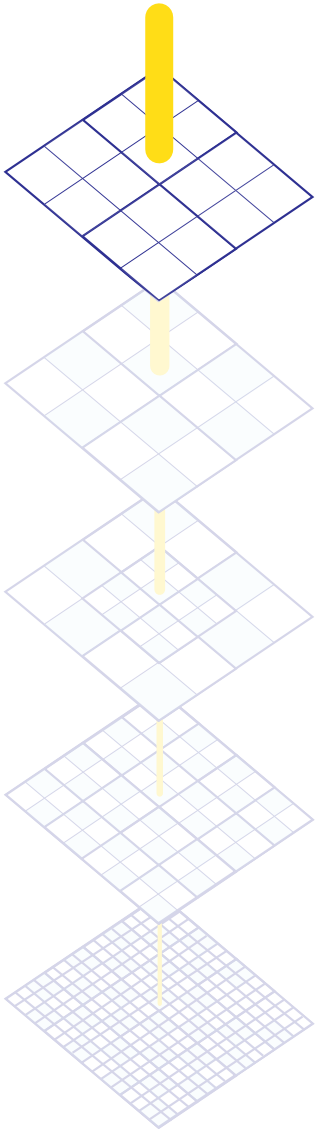
Examples of solid pieces of evidence include:

- a UK photocard driving licence
- an armed forces identity card
- a Northern Ireland electoral identity card
- a proof of age card recognised under PASS with a unique reference number
- a UK ePassport with biometric information
- identity cards from an EU or EEA country contain biometric information

How much evidence do I need?

That depends on how confident you wish to be in someone's identity. Generally, though, the stronger the evidence, the less required. Suppose your customer only has weak identity documents, such as bank statements or utility bills, that do not include an image of the claimed identity. In that case, your best practice is to collect multiple pieces of evidence.

STEP 1 - GET EVIDENCE OF THE CLAIMED IDENTITY



How to collect the evidence
An often overlooked part of a compliant ID verification process is how you actually collect the evidence.

There are several ways you can gather this evidence

- In-person
- By post
- Digitally
- By email
- Over the phone

The first two methods are fairly straightforward. Your customer could send you their ID documents through the post, bring them to a branch, or go to them. Either way allows you to confidently complete step 2, the verification of the documents.

Many businesses fail to comply with government guidance and best practices regarding the proceeding options.

GPG45 explicitly forbids accepting photos of the documents via Whatsapp / email or getting someone to flash their document up on screen during a video call as these methods do not allow you to confidently verify the documents.

In these cases, someone could send you a document that doesn't belong to them, obtain an image through a data breach or phishing scam, or use it without authorisation, such as a family member.

How Digital ID verification software helps
Digital verification software, especially those certified against the UK Government's Digital Identity and Attributes Trust Framework, has built-in protocols to capture evidence confidently.

These tools are capable of detecting whether

- The image is being captured in real-time
- The image is high enough resolution (making them easier to verify)
- The user is attempting to present an on-screen image
- The user is trying to present a printed replication

ID verification software can also use NFC technology to read the embedded chip in ePassports or other biometric documents, but this can only be achieved if the document is present.

Digital ID verification tools are also more convenient and faster than having to get a customer to bring their documents into branch or send through the post.

IDENTITY PROFILES

Before moving on to the next stage, let's address identity profiles/confidence levels. On the previous page, we discussed this concept several times and how, depending on the strength of the document, you can be more confident in the identity. The stronger the documents and the more verification steps you take, the higher the confidence level.

Why have different confidence levels?
You might be asking yourself why you have different levels of confidence. Shouldn't you always verify someone's identity to the highest level? Isn't that the safest and most reliable option? The answer is yes, but it's not always necessary.

The level you choose comes down to why you are verifying someone's identity and the risk it poses. If you are verifying someone's identity to help protect against fraud, then you may be comfortable with a lower level of confidence.

When confirming the Disclosure and Barring Service, for example, DBS insist on a Medium or High level of confidence as the data revealed is of a very-high sensitivity, and the potential to try to defraud is also high.

We must also consider accessibility/inclusivity and not make ID checks unnecessarily onerous. Not everyone has access to a biometric passport, so insisting on profiles that require very strong documents could exclude large proportions of the population.

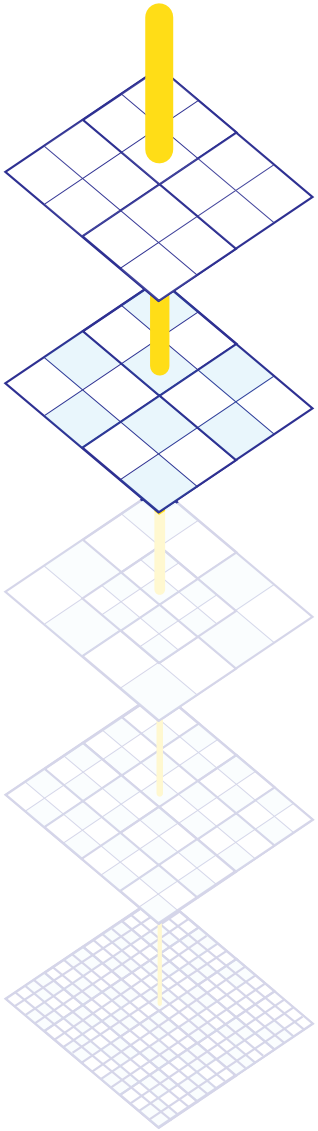
Confidence levels are calculated based on the strength of the document, the amount of evidence captured, and the additional verification methods used. Find our the full ID Profile Matrix in the appendices.

LOW
Typically involves basic checks using a single piece of evidence with little additional verification.

MEDIUM
Requires higher strength documents and / or additional verification such fraud or activity history.

HIGH
Requires higher strength documents and multiple verification checks, fraud checks and activity history.

VERY-HIGH
Requires higher strength documents and a combination of multiple verification checks, fraud checks and activity history.



STEP 2 - CHECK THE EVIDENCE IS GENUINE OR VALID

Now that you have the evidence, the next step is to check if it is genuine and whether you can rely on it.

To begin with, you should have a copy of a genuine, confirmed document against which to compare the evidence. You could use your own document if you have one, or most organisations will provide specimens for this purpose.

What to look for when verifying documents?

- Check that the document is genuine
- Check the physical security features
- Check for evidence of tampering
- Check for any irregularities/inconsistencies
- Check that the document hasn't expired

The "stronger" the document, the more certain you can be, as security features make it easier to verify. For example, a UK passport has several security features that are difficult to replicate or alter.

Weaker documents with fewer security features, like Bank Statements and utility bills, are easy to mimic and, therefore, more challenging to verify.

If you had a PDF of a Bank Statement bill, in order to verify its authenticity, you would need to obtain an official copy from the originating bank and then forensically review the document to see if there are any obvious attempts of tampering, such as changes to the layout, spelling mistakes, irregular font sizes, or inconsistent references.

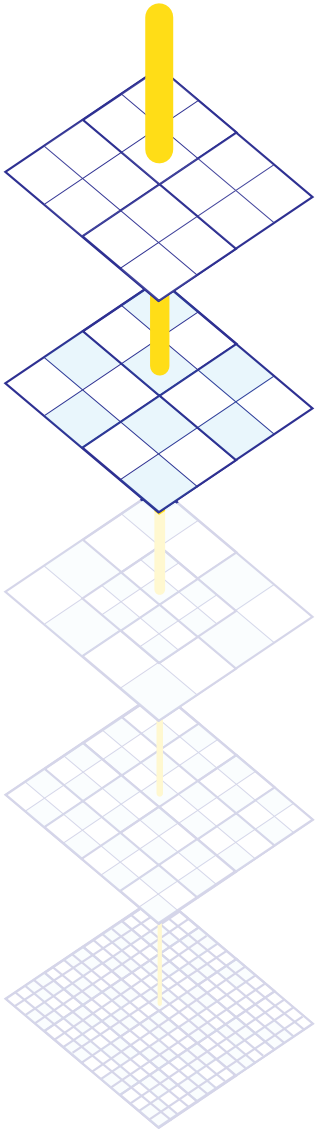
If checking in person, you MUST be checking the original document, not a scan or photocopy. For example, if a client brings in their ID, and your current process is to have a member of your front-office team photocopy the document to review at a later date. This is not compliant.

Dealing with expired documents

While you can accept expired documents, in most circumstances, they require additional validation as there may be more recent versions. It would help if you considered the length of time since the expiration and whether the information is still valid.

Expired documents are less likely to be monitored/ kept as securely by their original holders, and if the information is also out of date, attempts to misuse it may also go undetected.

STEP 2 - CHECK THE EVIDENCE IS GENUINE OR VALID



The benefits of Digital ID verification
Digital tools can instantly verify IDs, whereas manual verification can be time-consuming, prone to error and require expert training.

Advanced digital tools can use AI and machine learning to detect patterns and anomalies that indicate fraudulent activity, offering a higher level of protection against identity theft.

These tools have access to thousands of document libraries provided by official sources and can detect tampering at a pixel level, making them far more capable than human error.

Digital tools can also use the NFC technology built into modern smartphones to unlock the cryptographic chips within ePassports.

Another added benefit of digital ID verification is the secure storage of the documents and detailed metadata that can be easily provided as part of any audit process.

With manual checks, you are reliant on the individual to make detailed notes and store this information efficiently. For businesses that work across multiple locations, this can be very difficult, while a digital system centrally stores all data to the same standard, although you should always be aware of your data protection responsibilities

What type of checks do digital ID verification tools perform?

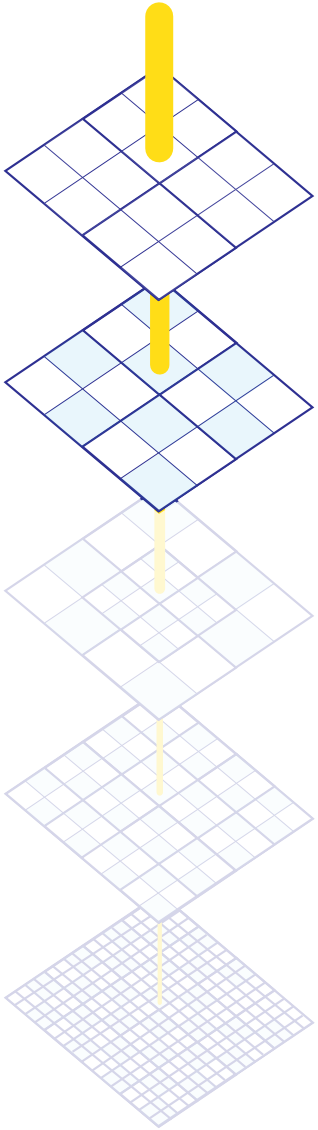
Template Matching & Consistency Checks
The tool compares the captured document against a database of known templates for thousands of ID document types sourced from trusted sources. This helps verify that the document conforms to the expected layout/format and looks for inconsistencies in information placement, fonts used, colours that conform to document templates, etc.

Security Feature Detection
The software will check for the presence and correct placement of holograms, watermarks, and other features such as micro-print / fine lines, which are difficult for the naked eye to detect.

Text Extraction and Validation
Most tools can also extract information within the document using Optical Character Recognition. This information can then be validated against known standards and formats.

Physical & Digital Tampering
Finally, advanced systems can examine the document for evidence of tampering. They will check for anomalies at a pixel level around the edges of the document and the photo, as well as inconsistencies in lighting/tones.

STEP 2 - CHECK THE EVIDENCE IS GENUINE OR VALID



Identifier-only checks

Some providers will ask an individual to provide an identity document identifier, such as the contents of the Machine-Readable Zone (MRZ) of a passport or the licence number on a driving licence, in order to validate these along with other personal details that appear on these documents.

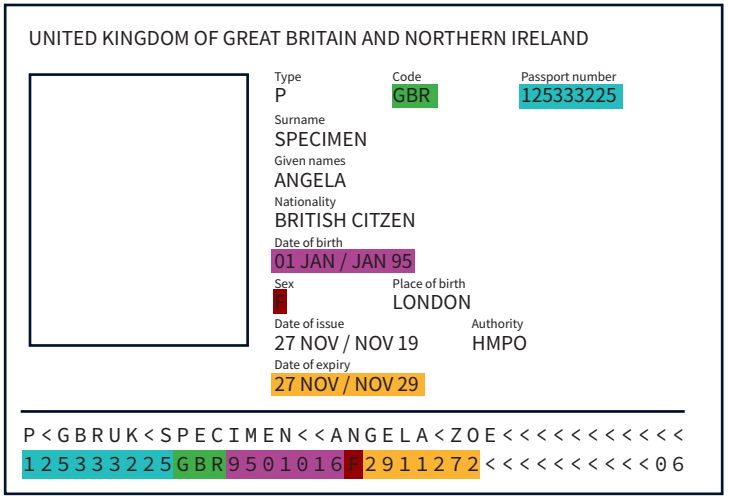
Some businesses believe this information is then checked against an official database, when in fact, the validation of these identifiers is purely algorithmic and simply confirms that the information provided is consistent with the format of the document.

The algorithms for both the MRZ of a passport and the licence number of a driving licence can be easily found online. However, they are open to abuse by fraudulent actors, and therefore, an algorithmic check alone cannot authenticate a document.

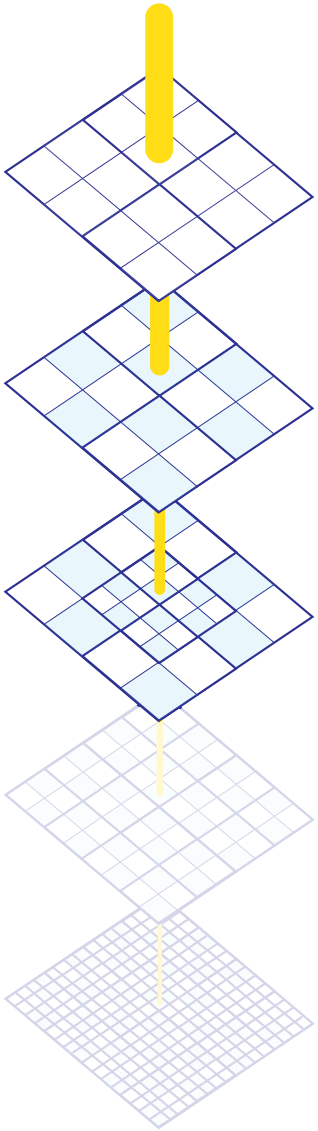
Even where an individual also provides an image of the passport (e.g. through email or instant messenger), this is insufficient as the UK Government's guidance on identity verification states:

"If the check is being done remotely, the image or video of the evidence must be clear enough for the system to examine its security features.

The image or video must be taken at the same time the check is being done. The user cannot upload an image or video of the evidence that they've taken before."



Here is an example a UK passport. If you examine the MRZ number closely you easily see how it a combination of the information above and can be easily replicated. Most MRZ checking service simply confirm this patten and do not perform any further verification checks.



STEP 3 - CHECK THE IDENTITY HAS EXISTED OVER TIME

The next step in the Government's recommended process is to check if the identity has existed over time, otherwise known as an activity check. By doing so, you lower the risk of accepting a synthetic ID or an identity belonging to someone deceased.

This step is optional in some circumstances and depends on strength of the evidence gathered and the level of risk involved in the transaction.

Imagine this scenario: a criminal sets up a new persona to hide their illegal gains. They set up utility bills, which do not require ID verification, in the name of their new identity and try to set up a bank account using these documents as evidence of their identity.

It is not uncommon for someone to have only low-strength forms of ID. Not everyone drives or has a passport. In order for the bank to verify the identity, they should take additional measures, such as an activity check, to establish that it is not a synthetic or fake ID.

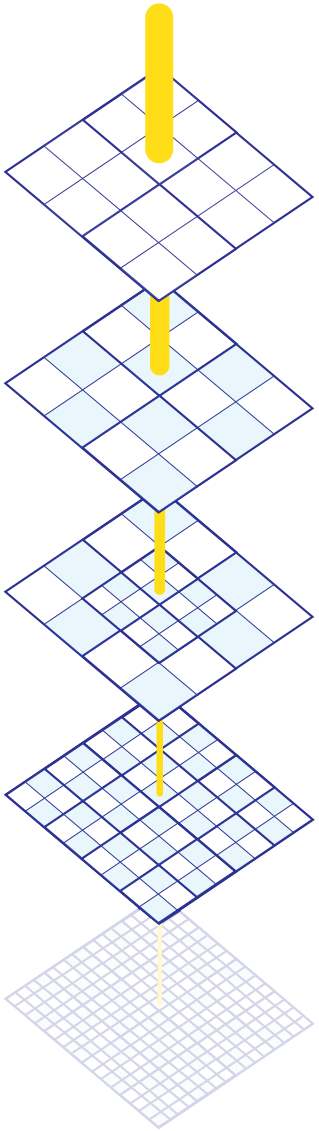
You may also be presented with a recently issued ID document and wish to verify that the identity has existed over time. The person could have changed their name by deed poll and be attempting to impersonate someone who has recently died in order to take control of their assets.

How to perform Activity Checks
Activity Checks are one of the more difficult tasks to complete and require the gathering of additional evidence to do so. If they are only providing utility bills, you could ask for documents that go back much further than your standard process.

You could also ask for certified copies of bank statements or use a compliance tool that utilises Open Banking to get verified digital statements.

You could also perform a full credit check on the customer. You will need their permission to do so, but the information provided will be able to provide robust evidence that the identity has existed over time.

How digital ID verification tools can help
Most ID verification tools will have some means to check someone's activity history. Most tools will be capable of running a soft credit check that confirms current and previous addresses as well as a high-level financial overview, such as when they opened their first bank account, evidence of credit cards, etc. Credit institutions are highly regulated and are regarded as trusted sources of information. Soft credit checks will show on the individual's credit file but do not impact their credit score and are therefore a quick way to confirm activity history without negatively impacting the individual.



STEP 4 - CHECK IF THE CLAIMED IDENTITY IS AT HIGH RISK OF FRAUD

You should verify a claimed identity using authoritative counter-fraud data sources to ensure that it is not at high risk of identity fraud or is suspected to be synthetic.

This process, known as an 'identity fraud' check, is essential for determining the risk associated with the claimed identity. This step is required if you are looking to achieve at least a medium level of confidence.

Examples of authoritative data sources include

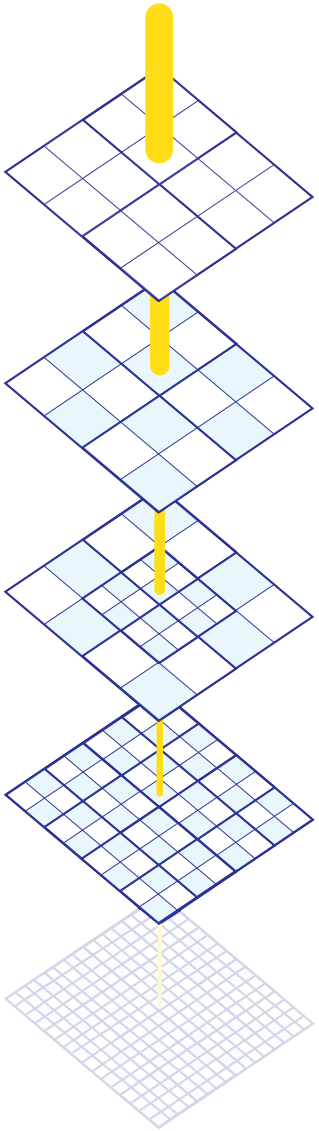
- CIFAS – a not-for-profit fraud prevention service in the UK
- Amberhill – a national fraud database managed by the Metropolitan Police
- HALO – UK mortality data
- Electoral roll – an official list of individuals who are eligible to vote in a particular jurisdiction
- Credit institutions – Large credit institutions hold extensive historical information on individuals regarded as trusted sources of information.

Anti-fraud databases such as Amberhill and CIFAS can provide information regarding whether an ID document has been reported lost, stolen, or suspected of being a victim of identity fraud. Access to these is usually via a specialist supplier or identity verification providers.

Verifying a claimed identity against multiple sources will reduce the risk of accepting fraudulent or synthetic IDs. This verification level provides the highest assurance of the claimed identity's validity and reduces the risk of fraud, as manipulating multiple authoritative sources is extremely difficult.

Suppose the data source does produce evidence that suggests the identity is at risk of fraud. In that case, further checks should be taken to verify the evidence collected as well as gather more evidence of the claimed identity.

STEP 4 - CHECK IF THE CLAIMED IDENTITY IS A HIGH RISK OF FRAUD



CAN YOU RELY ON DATA CHECKS ALONE?

Many ID verification providers offer a very basic digital check where you enter someone's name, date of birth, and address which are checked against some of the authoritative sources we've listed.

Whilst running an electronic check using a name, date of birth, and address may verify that an identity exists and it is not synthetic, it does not confirm that the provider of the details is the holder of the identity.

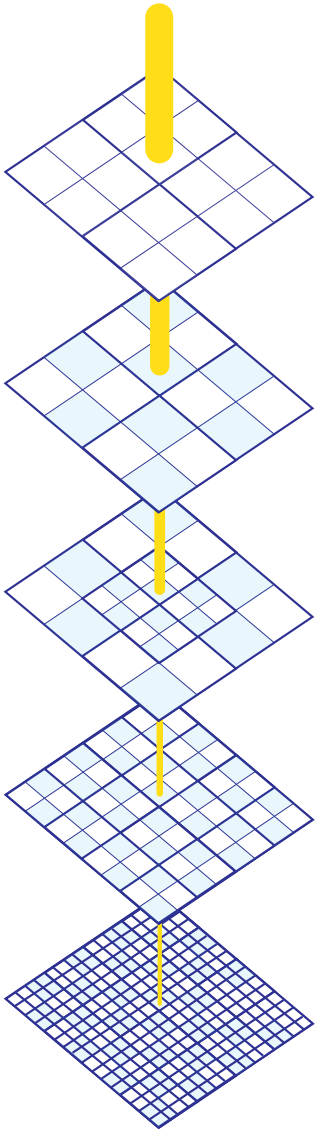
Furthermore, whilst the confirmed information may match what has been provided by the customer, this information is basic enough for anyone close to the claimed identity to mimic, making it less reliable. Data-only checks only really satisfy the fourth step of the Government's recommended stages and when used in isolation, exposes businesses to potential identity fraud.

Checking a claimed identity against authoritative sources will confirm it exists but shouldn't be used in isolation. Data checks reports are meant to support the evidence you've already gathered or used in conjunction with Knowledge Base Verification.

What are the risks associated with relying solely on data checks?

<u>Phishing & social engineering</u>
Phishing and social engineering continue to be threats to identity fraud and criminal activity. Criminals have become very capable of accessing someone's personal details, abusing this information to easily pass Knowledge-Based Verification and data-only ID checks. Imagine you're playing a game of Guess Who. You have a number of possible candidates in front of you. By running a data check, you are able to effectively eliminate other individuals and match against their information. With social engineering, the person on the other side of the board can see the same information and give you the answers you need.

<u>Family & close associates</u>
Family members and close associates are likely to have access to non-public information such as bank account details and previous addresses and can use this information to impersonate them. If you are relying on data checks and 'knowledge-based verification' without strong ID documents alone, you risk being victim to identity fraud



STEP 5 - CHECK THAT THE IDENTITY BELONGS TO THE PERSON

The last step is to prove that the person going through the identity verification process is connected with the evidence that has been gathered and verified.

If you collected strong evidence such as a passport or driving licence in step 1, then this step is pretty straightforward as you can compare the image on the document with the person in front of you.

When doing the match, you must ensure the identity of the person being checked is present. You can't, for example, rely upon a spouse to bring a copy of their partner's ID document as the comparison isn't taking place in person.

You can also perform this check remotely for certain use cases using video calls. Once again, you must ensure that the person is live and present, and you should rely on something other than previously recorded footage, as these can be easily tampered with or may have been provided without the person's permission.

How digital ID verification tools can help

Digital verification tools can match an individual to the document using advanced biometric facial recognition technology and ensure the person is 'live and present' when this happens.

What is biometric facial recognition?

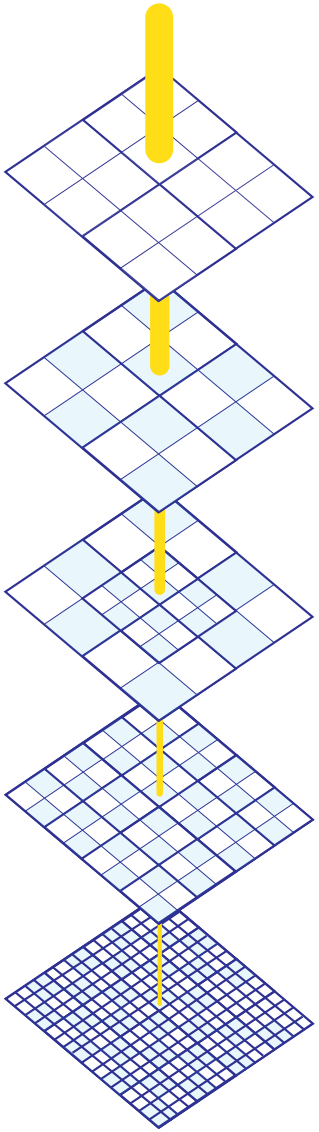
The process for the individual going through the ID check is very simple. It simply involves them taking a quick selfie—that's it, and it takes only a few seconds.

The software then takes these images and identifies key points on the face, known as landmarks. These can include the positions of the eyes, nose, mouth, and face contour. The software creates a digital vector of the face, mapping out the thousands of data points, calculating the distances between the eyes and mouth, the different ratios of the face, how the different landmarks align and many more micro measurements that are unique to the individual.

The software performs the same analysis on the image in the ID document and compares it to the two to determine whether they match.

By comparing thousands of data points, the software can also detect the use of facial masks or makeup to spoof the system.

STEP 5 - CHECK THAT THE IDENTITY BELONGS TO THE PERSON



What is liveness detection?

In remote identity verification, the use of liveness detection is critical in preventing presentation attacks or “spoofs”.

Common attacks include:

- presentation of printouts
- presentation of digital screens
- video playbacks
- facial masks

There are two forms of liveness detection: Active and Passive. Active Liveness is where a user is instructed to perform an action, such as tapping their nose or moving their head. By correctly performing this action, the user is considered as live and present.

Passive Liveness requires no instruction, command, or response from the user, giving no indication as to what security mechanism is being used, meaning they aren’t even aware a liveness check is taking place.

How is it possible to assess Liveness accurately from a single image when other solutions leverage full video?

Passive Liveness uses AI to determine whether an image taken is genuine or not using deep neural networks. Each neural network examines a different element of the image to detect artefacts that help distinguish between a photo of a live person and a presentation attack.

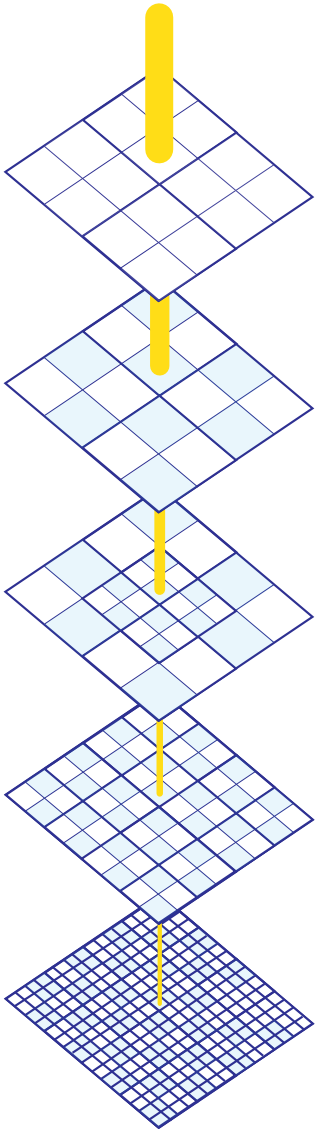
Other verification methods

An alternative method is to perform ‘knowledge-based verification’. Knowledge-based verification (KBV) is a method of identity verification that relies on a person’s knowledge of specific information, typically details associated with their personal history, such as addresses, phone numbers, or financial transactions.

However, KBV has become less favoured in recent years due to several drawbacks. Firstly, the proliferation of personal information on social media and other online platforms has made it easier for malicious actors to gather the necessary details for impersonation.

Additionally, as data breaches and identity theft incidents have increased, relying on static personal information for verification poses a significant security risk. These risks have prompted a shift towards more secure and dynamic methods, such as biometrics, to enhance the overall security of digital/remote interactions.

ONE FINAL STEP... RECORD KEEPING



By following these steps, you can protect your business from fraud, build trust with your clients, and ensure compliance with industry regulations. Let's make identity verification simple and effective together. Conducting compliant ID checks involves:

- Gathering strong evidence to begin with such as a passport or driving licence that have been issued by authoritative sources and have difficult-to-replicate security features
- Verifying the documents are genuine through trained manual checks or rely upon ID verification that has been certified against the UK government's Digital Identity and Attributes Trust Framework.
- Connecting the individual with the documents either in person by matching them with the photo in the ID document or using biometric facial recognition technology
- Using authoritative third-party sources to verify the information they have provided and check the identity has existed for over time and that there are no signs of fraud such as the claimed identity appearing in the HALO database.

Then, you can be confident that your customers are who they say they are.

One final but crucial step...

Criminals are becoming increasingly sophisticated and are aware of steps businesses are taking to spot and stop the use of fraudulent ideas. Regulators and law enforcement agencies do not anticipate businesses entirely eliminating the use of fake IDs. Instead, they expect businesses to implement consistent and thorough processes that minimise the risk of criminals and bad actors utilising fake IDs to further their illicit activities.

If someone does slip through the net, your only reprieve is the ability to demonstrate that you did all you could to try and prevent it. You should always keep robust and detailed records of the steps you take to complete your ID checks. In this aspect, digital ID verification is far superior to any manual method.

Automated systems reduce human error and ensure a consistent approach is always applied. Records can be easily retrieved and include comprehensive audit trails, documenting each step of the verification process, which aids in accountability and transparency.

APPENDICES

DOCUMENT STRENGTH LEVELS

LOW STRENGTH DOCUMENTS

- a Home Office travel document (convention travel document, stateless person's document, one-way document or certificate of travel)
- a birth or adoption certificate
- an older person's bus pass
- an education certificate from a regulated and recognised educational institution (such as an NVQ, SQA, GCSE, A level or degree certificate)
- a rental or purchase agreement for a residential property
- a proof of age card recognised under the Proof of Age Standards Scheme (PASS)
- a Freedom Pass
- a marriage or civil partnership certificate
- a gas or electric account
- a firearm certificate

HIGH STRENGTH DOCUMENTS

- passports that meet the International Civil Aviation Organisation (ICAO) specifications for machine-readable travel documents, such as a South African passport
- identity cards from an EU or European Economic Area (EEA) country that follow the Council Regulation (EC) No 2252/2004 standards
- UK photocard driving licences
- EU or EEA driving licences that follow the European Directive 2006/126/EC
- a Northern Ireland electoral identity card
- a US passport card
- a bank, building society or credit union current account (which the claimed identity can show by giving you a bank card)
- a student loan account
- a credit account
- a mortgage account (including buy to let mortgage accounts)

VERY HIGH STRENGTH DOCUMENTS

- biometric passports that meet the ICAO specifications for e-passports, such as a UK passport
- identity cards from an EU or EEA country that follow the Council Regulation (EC) No 2252/2004 standards and contain biometric information
- a UK biometric residence permit

IDENTITY PROFILE MATRIX

Profile	Evidence	Strength	Validity	Activity history	Identity fraud	Verification
L1A	1	2	2	N/A	1	1
L1B	1	3	2		1	1
L1C	1	1	1	3	2	2
L2A	2	1,1	1,1	2	1	2
L2B	2	1,1	1,1	2	2	2
L3A	1	1,1,1	1,1,1	2	1	1
M1A	1	4	2	N/A	1	2
M1B	1	3	2	1	2	2
M1C	1	3	3	N/A	N/A	3
M1D	1	2	2	2	1	3
M2A	2	2,2	2,2	3	2	2
M2B	2	3,2	2,2	1	1	2
M2C	2	3,2	2,2	N/A	1	3
M3A	3	2,2,2	2,2,2	2	2	2

IDENTITY PROFILE MATRIX

Profile	Evidence	Strength	Validity	Activity history	Identity fraud	Verification
H1A	1	4	3	N/A	1	3
H1B	1	3	3	2	1	3
H1C	2	4	3	N/A	N/A	4
H2A	2	2,2	2,2	3	3	3
H2B	2	4,3	2,2	N/A	2	3
H2C	2	3,2	3,2	1	1	3
H2D	2	3,3	3,2	N/A	1	3
H2E	2	4,3	3,3	N/A	N/A	3
H3A	3	2,2,2	2,2,2	2	2	3
V1A	1	4	3	N/A	3	3
V1B	1	4	4	N/A	1	3
V1C	1	4	3	1	1	4
V1D	1	4	4	N/A	N/A	4
V2A	2	3,3	3,3	3	2	3
V2B	2	4,3	3,3	N/A	2	3
V2C	2	4,2	3,2	2	2	3
V2D	2	4,4	4,4	N/A	N/A	3
V3A	3	3,2,2	3,2,2	3	3	3

CREDAS

sales@credas.com

02920 102 555

www.credas.com