GOV.UK

Guidance

How to prove and verify someone's identity

Updated 22 October 2020

Contents

Print this page

This publication is available at https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity

This guidance will help you decide how to check the identity of:

- a customer
- an employee
- someone acting on behalf of a business

You can check someone's identity:

- digitally
- over the phone
- by post
- by email
- face to face

By successfully checking users' identities, you can be confident that you'll give the right people the right things.

You might not always need to check someone's identity before you give them access to something. In some cases, you can just protect your service using 'authenticators' (https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services/giving-users-access-to-online-services).

You can also use this guidance to:

- understand how another individual or organisation checks someone's identity
- audit and certify identity products or services
- compare different identity checking processes with each other, for example schemes within the electronic identity and trust services (eIDAS) regulation (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN)

This guidance will not:

- tell you how to assess your risk of identity fraud
- be relevant if you ask users for information about their identity but do not check it (also known as 'self-assertion')

What is identity

An identity is a combination of characteristics that belong to a person.

A single characteristic is not usually enough to tell one person apart from another, but a combination of characteristics might be.

When to check someone's identity

You should check someone's identity if any services you or your organisation has will:

- show a user personal information about themselves, such as their driving licence or passport details
- give the user something

Why you should check someone’s identity

The number of identities being used to commit identity fraud in the UK is growing every year. Some of the most common reasons people or criminal groups commit identity fraud are to:

- access services they’re not entitled to
- get benefits they’re not entitled to
- steal personal, medical or financial information from other identities
- enable organised crime, like human trafficking
- avoid being detected by the police and other authorities

You could be affected by identity fraud if you do not check someone’s identity. This includes being targeted by someone:

- using a ‘synthetic’ (made up) identity
- who is pretending to be someone else (an ‘impostor’)

Synthetic identities can be fictional or based on a real identity. For example, someone who gives a false date of birth to access a gambling site is using a synthetic identity, even if their other details are correct.

If you follow this guidance, you’ll check identities in a way that’s consistent with other organisations or services that also follow it.

Checking identities in a consistent way reduces the chances of one organisation or service doing less effective identity checks than another. This means there are fewer organisations or services that could be targeted by identity fraud.

Checking identities in a consistent way means it’s also easier for you to trust and reuse an identity that’s been checked by someone else. This will mean:

- people have to prove their identity less often
- organisations and services can share the cost of checking someone’s identity

This does not mean you have to check an identity in exactly the same way as another organisation or service. You can do different types of checks but still have the same level of confidence in someone’s identity.

How to check someone’s identity

You’ll need to know the ‘claimed identity’ of the person you’re checking. A claimed identity is a combination of information (often a name, date of birth and address) that represents the characteristics of whoever a person is claiming to be.

When you have this information, you can find out if the person is who they say they are. This process is known as ‘identity checking’ and is made up of 5 parts:

- get evidence of the claimed identity
- check the evidence is genuine or valid
- check the claimed identity has existed over time
- check if the claimed identity is at high risk of identity fraud
- check that the identity belongs to the person who’s claiming it

You do not have to do all parts of the identity checking process at once. You can do them over any period of time and gradually build up your confidence in an identity.

You'll get a score for each part of the identity checking process you do. Do not add these scores up.

Levels of confidence

There are 4 different levels of confidence:

- low confidence
- medium confidence
- high confidence
- very high confidence

By reaching a level of confidence:

- you'll know how well your organisation or service is protected against identity risks
- your identity checking process can be understood and reused by other organisations and services

You can reach a level of confidence by meeting an identity profile (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-profiles). The results of your service's risk assessment will help you decide which level to meet. You should aim to get a higher level of confidence in someone's identity if you or your service are at high risk of identity-related crime.

Your confidence in someone's identity can increase over time if you do extra checks or collect more evidence.

It can also decrease over time, for example if you later find out that evidence you used was lost or stolen at the time you checked that person's identity.

You can also reuse identity checks done by another organisation if they do some or all parts of the identity checking process explained in this guidance.

Low confidence in someone's identity

Compared to not doing any identity checks, having low confidence in someone's identity will lower the risk of you accepting either:

- synthetic identities
- impostors who do not have a relationship with the claimed identity

Medium confidence in someone's identity

Having medium confidence in someone's identity will protect you against the same things as low confidence. It will also lower the risk of you accepting impostors who have information about the claimed identity that's not in the public domain.

For example, it would protect you against someone who works for the claimed identity's employer's HR department from using any information they have to impersonate the claimed identity.

High confidence in someone's identity

Having high confidence in someone's identity will protect you against the same things as medium confidence. It will also lower the risk of you accepting impostors who:

- know the claimed identity (this includes their close friends or family)
- do not match the claimed identity's photo or biometric information

Very high confidence in someone's identity

Having very high confidence in someone's identity will protect you against the same things as high confidence. It will also lower the risk of you accepting impostors who are trying to look like the claimed identity, for example by wearing a mask or make up.

Authoritative sources

You might need to check things with an 'authoritative' source. To be authoritative for a particular piece of information, the source must make sure:

- the integrity of the information is protected
- the information is up to date

The source must also do one of the following:

- issue evidence, for example the Driver and Vehicle Licensing Agency (DVLA) issues evidence such as driving licences
- get information from an organisation that issues evidence, for example credit reference agencies can have authoritative information about bank accounts
- get information from another authoritative source, for example from another identity scheme

Get evidence of the claimed identity

You can collect:

- physical evidence of the claimed identity (such as an identity document, like a passport)
- digital evidence of the claimed identity (such as information from a personal data store)

You can ask the user to provide the evidence or you can find it yourself, for example by checking a database. If you want to find the evidence yourself, you will need enough information about the claimed identity to be able to match it to their records.

This will prove that the identity exists, but it does not prove that it belongs to the person who's claiming it. You must do a verification check to find that out.

You can also accept and score a declaration from someone that knows the claimed identity (https://www.gov.uk/government/publications/how-to-accept-a-vouch-as-evidence-of-someones-identity) (known as a 'vouch') as evidence.

Some types of evidence are 'stronger' than others, which means they will be harder to:

- forge (when existing evidence is changed to make it look like it belongs to someone else)
- counterfeit (when evidence is created from scratch)

You can check how strong evidence is by finding out:

- what security features protect it (for example a hologram or an electronic chip)
- what information it has
- how the person's identity was checked when the evidence was issued

You must check and score one piece of evidence at a time. Do not add these scores up.

This is also known as a 'strength' check.

The stronger the evidence is, the higher its score will be. The highest score you can get for this part of the identity checking process is 4.

If the user has changed their name

There are a number of reasons why someone's name might be different on different pieces of evidence. For example, their surname might have changed when they got married.

If it looks like someone has changed their name, you might need to collect more evidence to make sure the evidence belongs to the same person. The combination of evidence you collect must match an identity profile for the level of confidence you need.

You should be aware that some users might have changed their name because of gender reassignment. If this happens, you must make sure you comply with section 7 of the Equality Act 2010 (https://www.legislation.gov.uk/ukpga/2010/15/section/7) when you ask them for any evidence that includes their previous names.

The identity is also sometimes shown as a synonym on different pieces of evidence. For example, it might say the person's name is Samantha on their passport, but Sam on their bank card.

You can usually accept a synonym unless you need to know the claimed identity's 'official name'. This is the name on any official documents they have, such as their passport.

Transposition errors

Other information might appear to be different on different pieces of evidence. These mistakes are known as 'transposition errors'.

This can happen with:

- names that have multiple parts, for example 'Anna-Marie Jane' might appear as 'Anna Marie-Jane'
- days and months in dates, for example '08.10.1978' might appear as '10.08.1978'
- centuries in dates, for example '1998' might appear as '1898'
- addresses, for example 'Flat 1a, 29 Acacia Road' might appear as 'Flat 29a Acacia Road'

These mistakes will not usually affect how you do this part of the identity checking process.

Score 1

The evidence will have a score of 1 if it contains 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 characteristics, like an iris or fingerprint)
- a photo of the claimed identity
- a reference number

The evidence should come from an organisation or person that you know will:

- check the claimed identity when they issue the evidence
- make sure its process for issuing the evidence is not misused

Some examples of evidence that will have a score of 1 include an email, PDF or letter from a local authority.

You may not be able to thoroughly check the validity of any evidence that has a score of 1.

Score 2

The evidence will have a score of 2 if it has everything it needs to get a score of 1 and includes information that's unique to either:

- the identity (for example the name and a photo of the claimed identity)
- that piece of evidence (for example a reference number)

The organisation that issued the evidence must follow a published policy when checking the claimed identity.

If the evidence includes a name, it must show the person's full name instead of any pseudonyms, aliases or nicknames.

If the evidence is a physical document, it must be protected by physical security features. These features will stop it from being reproduced without specialist knowledge or information.

If the evidence includes digital information, it must either be protected by:

- cryptographic security features that correctly identify the person or organisation that issued it
- processes that make sure only authorised users can create, update and access it

Some examples of evidence that have a score of 2 include:

- 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
- a ‘substantial’ electronic identity (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R1502&from=EN)’ from a notified eIDAS scheme (https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS)

Score 3

The evidence will have a score of 3 if it has everything it needs to get a score of 2 and:

- it includes information that’s unique to both the identity and that piece of evidence
- whoever issued the evidence made sure it was received by the same person who applied for it, for example it could be sent by secure delivery
- whoever issued the evidence checked the claimed identity in a way that follows a standard or regulation that’s been approved or recognised by the UK government, such as the Money Laundering Regulations 2017 (https://www.legislation.gov.uk/uksi/2017/692/made)

It must also:

- include the person’s official name instead of their initials or synonyms, for example ‘Julian’ instead of ‘Jules’ (if the evidence includes a name)
- be protected by physical security features that stop it from being reproduced without specialist equipment (if the evidence is a physical document)

The evidence must also include one of the following:

- a photo of the person
- biometric information that uses cryptographic security features to protect its integrity
- cryptographic security features that can be used to identify the person who owns the evidence (this includes evidence with cryptographic chips and digital accounts that are protected by cryptographic methods)

Some examples of evidence that will have a score of 3 include:

- passports that meet the International Civil Aviation Organisation (ICAO) specifications for machine-readable travel documents (https://www.icao.int/publications/pages/publication.aspx?docnum=9303), 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 (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32004R2252)
- UK photocard driving licences
- EU or EEA driving licences that follow the European Directive 2006/126/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0126)
- 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)
- a digital tachograph driver smart card (https://www.gov.uk/apply-for-a-digital-tachograph-driver-smart-card)
- an armed forces identity card
- a proof of age card recognised under PASS with a unique reference number
- a loan account (including hire purchase accounts)
- a 'high (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R1502&from=EN)' electronic identity from a notified eIDAS scheme (https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS)

Score 4

The evidence will have a score of 4 if it has everything it needs to get a score of 3 and:

- it includes biometric information
- all digital information (including biometric information) is protected by cryptographic security features
- the cryptographic security features can prove which organisation issued the evidence
- whoever issued the evidence proved the claimed identity by comparing and matching the person to an image of the claimed identity from an authoritative source

Some examples of evidence that will have a score of 4 include:

- biometric passports that meet the ICAO specifications for e-passports (https://www.icao.int/publications/pages/publication.aspx?docnum=9303), such as a UK passport
- identity cards from an EU or EEA country that follow the Council Regulation (EC) No 2252/2004 standards (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32004R2252) and contain biometric information
- a UK biometric residence permit (https://www.gov.uk/biometric-residence-permits)

Check the evidence is genuine or valid

If you want to prove someone's identity using information that's on physical evidence, you must check it's genuine. This means that the evidence is unlikely to be forged or counterfeit.

Example You could use a PASS card to prove the name and date of birth of the claimed identity. You will need to check the physical security features on the PASS card to do this.

If you're using digital evidence, you must check the cryptographic security features instead.

Example You could use information from a personal data store to prove the address of a claimed identity. You will need to check that the information is protected by cryptographic security features that can tell you who created the information. You must also check that the information has not been tampered with.

You can also check that the evidence:

- is valid (this means you can find records that show the evidence has been issued)
- has not expired
- has not been cancelled or reported as lost or stolen

This is also known as a ‘validity’ check.

You can check the evidence in person or remotely.

The highest score you can get for this part of the identity checking process is 4.

Score 1

The evidence will have a score of 1 if it appears to be genuine.

The person checking the evidence must be able to confirm:

- they’re checking an original, certified copy or scan of the evidence
- there are no errors on the evidence, like wrong paper type, spelling mistakes, irregular use of fonts or missing pages
- the details, layout or alignment of the evidence look the way they should
- any logos look the way they should
- any references to information are the same across the evidence (for example if the body text of a letter references an address, this should match the address shown at the top of the letter)

Score 2

The evidence will have a score of 2 if you make sure it has not expired and you can confirm any of the following:

- the evidence is valid
- the visible security features are genuine (these are security features that can be seen without using specialist light sources)
- the ultraviolet (UV) or infrared (IR) security features are genuine

Confirm the evidence is valid

The person or system doing the check can confirm the evidence is valid by making sure the details on it match those held by an authoritative source.

Confirm the visible security features are genuine

If the evidence is being checked in person, whoever is doing the check must make sure:

- the original evidence has been shown
- they do not accept scans, photos, or photocopies of the evidence (this is because it can be difficult to tell if these have been forged or counterfeit)

The evidence must always be shared in a way that protects it from being tampered with. For example, it could be sent by secure delivery if it’s being checked in person.

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.

They should check this using non-specialist light sources such as natural sunlight, indoor lights or desk lamps.

The person or system will need to use official templates to check any of the following features on the evidence look the way they should:

- background printing
- fonts and alignment
- holograms and positioning
- the way it's been laminated
- designs printed with optical variable ink (and check they look the way they should at certain angles)
- the format of any 'compound identifiers', such as a Driver and Vehicle Licensing Agency (DVLA) driver number or a machine-readable zone (MRZ)
- the position of any photographs on the evidence (they should not have been replaced or edited)

Some places where you can find official templates are:

- the Public Register of Authentic travel and identity Documents Online (https://www.consilium.europa.eu/prado/en/search-by-document-country.html) (PRADO)
- the EU and EEA driving licence handbook (https://op.europa.eu/en/publication-detail/-/publication/ae58b7c9-4716-46e2-8868-2920735bc95d)
- EdisonTD (http://www.edisontd.net/)

If the evidence is being checked by a person, they must:

- be trained in how to detect false documents by a specialist trainer, such as the Home Office, National Document Fraud Unit or Centre for the Protection of National Infrastructure (CPNI)
- refresh their training at least every 3 years

If the evidence is being checked by a system, it must:

- have been built following good practice, such as the Home Office's guidance on identification document validation technology (https://www.gov.uk/government/publications/identity-document-validation-technology/identification-document-validation-technology)
- update the templates it checks the evidence against at least every 3 years

Confirm the UV or IR security features are genuine

The person or system doing the check will need to use a UV or IR light to make sure:

- the paper the evidence is printed on looks the way it should
- the alignment of the evidence looks the way it should
- any fluorescent features (such as fluorescent inks or fibres) look the way they should

- the evidence has not been tampered with (for example a UV light will show where UV features have been covered by glue if something has been stuck on the evidence)

The person or system will need to use official templates to check any of the following features on the evidence look the way they should:

- background printing
- fonts and alignment
- holograms and positioning
- the way it's been laminated
- designs printed with optical variable ink (and check they look the way they should at certain angles)
- the format of any 'compound identifiers', such as a DVLA driver number or a MRZ
- the position of any photographs on the evidence (they should not have been replaced or edited)

Some places where you can find official templates are:

- PRADO (https://www.consilium.europa.eu/prado/en/search-by-document-country.html)
- the EU and EEA driving licence handbook (https://op.europa.eu/en/publication-detail/-/publication/ae58b7c9-4716-46e2-8868-2920735bc95d)
- EdisonTD (http://www.edisontd.net/)

If the evidence is being checked by a person, they must:

- be trained in how to detect false documents by a specialist trainer, such as the Home Office, National Document Fraud Unit or CPNI
- refresh their training at least every 3 years

If the evidence is being checked by a system, it must:

- have been built following good practice, such as the Home Office's guidance on identification document validation technology (https://www.gov.uk/government/publications/identity-document-validation-technology/identification-document-validation-technology)
- update the templates it checks the evidence against at least every 3 years

Score 3

Any evidence protected by cryptographic security features will have a score of 3. You must make sure these security features are genuine.

The evidence can also have a score of 3 if you do all of the following:

- confirm the evidence is valid or check the evidence has not been cancelled, lost or stolen
- confirm any physical security features are genuine
- check the evidence has not expired

Confirm the cryptographic security features are genuine

To make sure the cryptographic security features are genuine, the system that checks the evidence will need to:

- read the cryptographically protected information
- provide any required cryptographic keys
- check the evidence has not expired
- check the digital signature is correct

It will also need to check the signing key:

- belongs to the organisation that issued the evidence
- is the correct type for that evidence
- has not been revoked

Example Most debit or credit cards will have a cryptographic chip on them. You can check the chip is genuine by asking a user to make a zero balance payment using a card reader. If the transaction is successful you'll know the cryptographic chip and the bank account linked to it are genuine.

Confirm the evidence is valid

The person or system will need to do the same checks to confirm the evidence is valid that are needed at score 2.

Check the evidence has not been cancelled, lost or stolen

The person or system doing the check will need to make sure the evidence has not been:

- cancelled by the organisation that issued it
- reported as lost or stolen

They can do this by checking an authoritative database of cancelled evidence, for example Interpol for passports or a mobile phone operator for mobile phone contracts.

Confirm any physical security features are genuine

The person or system must do the same things needed at score 2 to confirm any visible security features are genuine. They must also confirm that any UV or IR security features are genuine.

They'll also need to:

- use evidence that has not been intercepted and reused (known as a 'replay attack')
- make sure any shadows or glare do not stop the security features on the evidence from being examined
- update any official templates that are used (such as those from PRADO) every year
- refresh their training in how to detect false documents every year (if the checks are being done by a person)

They must also confirm any:

- designs printed using intaglio (raised) ink look the way they should
- designs that have been laser etched look the way they should

- features are consistent and correct across sections of the evidence

Example In a UK passport, there should be a passport number on the page with the person's details on it. You should check if this number is the same as the number punched on the other pages in the passport.

To check this, they must use one of the following:

- a magnification tool, such as a magnifier
- other inspection equipment used to identify forged or counterfeit documents, such as a UV light

Score 4

The evidence will have a score of 4 if you do all of the following:

- confirm the visible security features are genuine
- confirm the UV or IR security features are genuine
- confirm the cryptographic security features on the evidence are genuine
- check the evidence has not been cancelled, lost or stolen
- check the evidence has not expired

Confirm the visible security features are genuine

The person or system must do the same things needed at score 3 to confirm the visible security features are genuine.

They'll also need to:

- be supervised when they capture and examine the evidence by someone who's also been trained by a specialist trainer, such as the Home Office, National Document Fraud Unit or CPNI
- examine the evidence under 'controlled' light conditions (this means the lighting in the room creates the best possible environment for examining the security features on the evidence)
- examine the evidence under 'controlled' security conditions (this means there are ways to prevent systems from being fooled or people from being manipulated)

They'll need to check the following features of the evidence look correct:

- watermarks
- security fibres
- consistency throughout the evidence
- secondary background ('ghost') images

Example In the latest UK passport, there should be a ghost image of the person on the 'observations' page. You should check if the surname and date of birth in the image are the same as the person's details.

To check this, they must use one of the following:

- a magnification tool (such as a magnifier)
- a low angle ('oblique') light

- other inspection equipment to identify forged or counterfeit documents

Confirm the UV or IR security features are genuine

The person or system must do the same things needed at score 3 to confirm any UV or IR security features are genuine.

Confirm the cryptographic security features are genuine

The person or system must do the same things needed at score 3 to confirm the cryptographic security features are genuine.

Check the evidence has not been cancelled, lost or stolen

The person or system must do the same things needed at score 3 to confirm the evidence has not been cancelled, lost or stolen.

Check the claimed identity has existed over time

You should check the claimed identity has existed over time. This will lower the risk of you accepting either:

- a synthetic identity
- an identity that belongs to someone who's died

This is also known as an 'activity history' check.

You do not need to do this part of the identity checking process to meet all the identity profiles.

The highest score you can get for this part of the identity checking process is 4.

You should check if there are records that show the claimed identity has regularly interacted with other organisations or people. How many interactions you need to find will depend on if the organisation or person did an identity check during the interaction.

Some examples of interactions include:

- credit card transactions
- gas or electricity account payments
- someone signing in to an online bank or retail account
- someone travelling to another country
- health records
- employment records
- school records

You can also accept a vouch (https://www.gov.uk/government/publications/how-to-accept-a-vouch-as-evidence-of-someones-identity) from someone who knows the claimed identity as proof they've existed over time.

How confident you can be that the claimed identity was involved in these interactions depends on if their identity was checked by the organisation or person they interacted with.

Find out what identity checks have been done

Different types of organisations and people will check identities in different ways.

Not everyone will check someone's identity when they interact with them. If you cannot find out what sort of identity checks they do, you can assume they do not do any. This means you will need to look for more interactions over a longer period of time.

You're likely to find records of interactions between claimed identities and the following types of organisations. They might interact with other organisations that do identity checks in a different way.

Educational organisations

You might find interactions between the claimed identity and an educational organisation, such as a school or college. You can be sure these types of organisations will have done some basic identity checks.

Financial organisations

You might find interactions between the claimed identity and a financial organisation, such as a bank or credit agency. You can be sure these types of organisations will have checked identity in a way that meets the requirements of the Money Laundering Regulations 2017 (https://www.legislation.gov.uk/uksi/2017/692/contents/made).

Travel companies or border or immigration authorities

You might find interactions that show the claimed identity has travelled to another country. Their identity will have either been checked by the company they travelled with, such as an airline, or by a border or immigration authority. The claimed identity's physical appearance or biometric information would have been compared to an official identity document, such as a passport.

Scores

The score you'll get will depend on:

- what type of identity checks the organisation or person did
- when the interactions you found took place

You'll get a higher score if the identity has existed for a long time or it has been checked more thoroughly.

	Interactions over the last 3 months	**Interactions over the last 6 months**	**Interactions over the last year**	**Interactions over the last 2 years**	**Interactions over the last 3 years**
Identity was not checked	N/A	N/A	Score 1	Score 2	Score 3
Identity was checked following a published policy	Score 1	Score 2	Score 3	Score 4	Score 4

	Interactions over the last 3 months	Interactions over the last 6 months	Interactions over the last year	Interactions over the last 2 years	Interactions over the last 3 years
Identity was checked following the Money Laundering Regulations	Score 2	Score 3	Score 4	Score 4	Score 4
Physical appearance or biometric information was checked against an official source	Score 3	Score 4	Score 4	Score 4	Score 4

Check if the claimed identity is at high risk of identity fraud

You should make sure the claimed identity is not at a higher than usual risk of identity fraud or likely to be synthetic.

You can do this by checking the details of the claimed identity with authoritative counter-fraud data sources, such as a national fraud database.

This is also known as an ‘identity fraud’ check.

You do not need to do this part of the identity checking process to meet all the identity profiles.

The highest score you can get for this part of the identity checking process is 3.

Score 1

You’ll get a score of 1 if you use an authoritative source to check if the claimed identity has either:

- had its details stolen (even if those details have not been used fraudulently yet)
- been reported as stolen

If either of these things have happened, you must do extra ‘verification’ checks.

You must also use an authoritative source to check if the claimed identity is a known synthetic identity.

If it is, you must reduce these risks by:

- doing additional verification checks
- collecting more evidence of the claimed identity

Score 2

To get a score of 2 you must do all the checks needed to get a score of 1. You must also use an authoritative source to check that the claimed identity:

- belongs to someone who’s still alive

- is known by an organisation that should have a record of that person (for example an Electoral Registration Office in a local authority)
- is at a usual risk of being impersonated (for example a ‘politically exposed person’ like a politician or judge is at a higher than usual risk of being impersonated)

You must do extra ‘verification’ checks if you get any information from the authoritative source that suggests these things are not true.

Score 3

You’ll get a score of 3 if you use more than one authoritative source to do all the checks needed to get a score of 2.

The sources must also be ‘independent’, which means they’re either:

- separate from the part of your organisation that checks the person’s identity
- part of a different organisation

Check that the identity belongs to the person who’s claiming it

You must prove that the person who’s going through your identity checking process is the claimed identity. You might let someone access your service using a claimed identity that belongs to someone else if you do not do this.

This is also known as a ‘verification’ check.

The highest score you can get for this part of the identity checking process is 4.

Score 1

The person will get a score of 1 if they can prove they know information that does not change over time (‘static’ information) that only the claimed identity should know.

You should check this by asking the person to complete ‘knowledge-based verification’ (KBV) challenges.

You can do this using:

- a free text response, where they can answer in any way they like
- multiple choice, where they can choose an option from a set of possible answers that you provide

It’s usually more difficult for an impostor to complete a free text challenge than a multiple choice challenge. This is because they might be able to guess the right answer when completing a multiple choice challenge.

If you decide to accept free text responses to KBV challenges, be aware that they might include spelling mistakes or other errors. This can sometimes make it harder to match the responses to a record.

Example You can ask the person to give you a customer reference number that was issued to them when they bought something from your organisation. They will need to type this into a free text field. You can make sure the number was issued to their claimed identity by checking it against your

records. This reference number is static because it does not change over time.

How many KBV challenges you ask the person to complete depends on:

- if the challenges are low, medium or high quality
- the way the person completes the challenge

You should ask the person to complete one of the following:

- 2 low quality free text KBV challenges
- 4 low quality multiple choice KBV challenges
- 1 medium quality free text KBV challenge
- 2 medium quality multiple choice KBV challenges
- 1 high quality free text KBV challenge
- 1 high quality multiple choice KBV challenge

Quality rules for KBV challenges

KBV challenges should be specific enough to be able to prove that that person is who they say they are.

Someone who has stolen a claimed identity's wallet, purse or phone should not be able to complete all of the KBV challenges you ask them to.

Low quality KBV challenges must be:

- about the claimed identity
- clear and simple so the person knows exactly what you're asking them
- about something the claimed identity can reasonably be expected to know
- from a source that maintains the integrity of the information the question is based on
- from a source that makes sure the information cannot be misused by the claimed identity (for example the claimed identity should not be able to create false records)

Low quality KBV challenges must not:

- be able to be answered with information that's available in the public domain (for example in an open dataset or on a website that anyone can access)
- be able to be answered using information the person has submitted at another point in the identity checking process
- be predictable (the questions and answers should change each time someone goes through your identity checking process)
- have answers that can be easily guessed if you're asking multiple choice questions
- include information that will give the person the answer to another question
- show personal information (unless the person has already submitted it at another point during the identity checking process)

Medium quality KBV challenges must meet all the requirements for low quality challenges, as well as:

- be based on information from a source that did its own identity checks on the claimed identity

- share codes, like a one-time password sent to the claimed identity's phone, in a way that means you can be sure they were given to the claimed identity (if you use them)

High quality KBV challenges must meet all the requirements for low and medium quality challenges. They must also be based on information:

- from a source that checked the claimed identity was who they said they were in a way that follows the Money Laundering Regulations 2017 (http://www.legislation.gov.uk/uksi/2017/692/made)
- from a source that makes sure the information cannot be accessed, modified or created by its employees
- from a source that's separate from your organisation
- from a source that's regulated by a statutory or independent body
- that cannot be known or accessed by anyone apart from the claimed identity and their immediate family without breaking the law (for example you should not use information that you know is available on the dark web)

Score 2

The person will get a score of 2 if you do one of the following:

- make sure the person physically matches the photo on or associated with the strongest piece of genuine evidence you have of the claimed identity (you can do this in person or remotely)
- make sure the person's biometric information matches biometric information from the strongest piece of genuine evidence you have or an authoritative source
- ask the person to complete multiple 'dynamic' KBV challenges that only the claimed identity should be able to do

Make sure someone matches the photo in person

The person doing the match must:

- have been trained in how to detect impostors by a specialist trainer, such as the Home Office, National Document Fraud Unit or CPNI
- refresh their training at least every 3 years
- have good enough eyesight (with or without prescription lenses) to effectively compare the person to the image

When doing the match, you must make sure:

- the person whose identity is being checked is present
- the light conditions are good enough to clearly see the person and the image on the evidence (for example there should be no glare or shadows)
- you are comparing the person to a photo from genuine evidence
- the photo has not been tampered with

The person whose identity is being checked must not:

- be wearing a head covering (unless it's for religious or medical reasons)

- have their eyes closed
- have anything covering their face or eyes (such as shadows or their hair)

If someone is wearing a face covering to help prevent the spread of coronavirus (https://www.gov.uk/government/publications/face-coverings-when-to-wear-one-and-how-to-make-your-own/face-coverings-when-to-wear-one-and-how-to-make-your-own), you can ask them to take it off to be identified. You can also choose to check they match the photo remotely instead.

Make sure someone matches the photo remotely

When doing the match, you must make sure:

- the person whose identity is being checked is present when their image or video is captured (you should not use a scan or an upload from a photo or video feed)
- the image or video has not been intercepted and reused (‘replayed’)
- you are comparing an image or video of the person to an image or video of genuine evidence
- the image or video has been shared in a way that prevents it from being tampered with (for example by using a ‘man-in-the-middle’ attack)

If a person is doing the match, they must:

- have been trained in how to detect impostors by a specialist trainer, such as the Home Office, National Document Fraud Unit or CPNI
- refresh their training at least every 3 years
- have good enough eyesight (with or without prescription lenses) to effectively compare the person to the image

The image or video of the person must be:

- clear and in focus
- in colour

In the image or video, the person must:

- be in clear contrast to the background
- not have ‘red eye’
- not wear a head covering (unless it’s for religious or medical reasons)
- not have their eyes closed
- not have anything covering their face or eyes (such as shadows or their hair)

Make sure someone matches biometric information

When doing the biometric comparison, you must make sure:

- the number of ‘false matches’ and ‘false non-matches’ (https://www.ncsc.gov.uk/collection/biometrics?curPage=/collection/biometrics/measuring-performance) in your system are appropriate for your security and usability needs
- your system matches the person to biometric information that’s known to belong to the claimed identity (this is known as ‘one-to-one verification’)

- the biometric information has not been tampered with (if it was taken from a piece of evidence)
- your system can identify if the person's biometric information has been intercepted and reused ('replayed')
- the biometric information has been shared in a way that prevents it from being tampered with
- your system can tell if someone's using an artefact to convince the system they're someone else (known as 'spoofing') - this could mean making sure they're not holding up a photo or playing a recording of someone's else's voice if you're checking a facial or vocal type ('modality') of biometric
- your system confirms that the person is real (known as a 'liveness' test)

Example If you're checking a fingerprint biometric modality, you can use heart rate sensors to make sure that the person who is providing their fingerprint is alive.

Asking the person to complete dynamic KBV challenges

To be 'dynamic', the answers to a KBV challenge must change over time. This will make it harder for impostors using information from things like data breaches to successfully complete the challenge.

The KBV challenges must follow the same quality rules that need to be followed to get a score of 1.

The KBV challenges must also not be based on information from a single source. An account and a mortgage from the same bank count as different sources if the claimed identity went through a different application process to get each one.

Example You can make a zero balance transaction into the claimed identity's bank account and attach a reference number (which is valid for a short period of time) to it. This will show up as a code on the claimed identity's bank statement.

The person will need to sign in to the claimed identity's account within the allowed time to get the code. If they give you the correct code, it will prove the person you're dealing with has control of and access to that account. Only the claimed identity should be able to do this.

You can ask a combination of different quality KBV challenges to get a score of 2.

Some of the following combinations require you to ask the person to complete multiple choice challenges. Wherever this is an option, you can choose to ask the person to complete free text challenges instead. This is because free text challenges are better at catching out impostors who might pretend to be the claimed identity.

If you ask 1 high quality free text challenge, you must also ask at least one of the following:

- 2 low quality multiple choice challenges
- 1 low quality free text challenge
- 1 medium quality multiple choice challenge

If you ask 1 high quality multiple choice challenge, you must also ask at least one of the following:

- 3 low quality multiple choice challenges
- 2 low quality free text challenges
- 1 low quality free text challenge and 1 low quality multiple choice challenge
- 1 medium quality multiple choice challenge

If you ask 1 medium quality free text challenge, you must also ask at least one of the following:

- 4 low quality multiple choice challenges
- 2 low quality free text challenges
- 1 low quality free text challenge and 2 low quality multiple choice challenges
- 1 medium quality multiple choice challenge and 1 low quality multiple choice challenge
- 2 medium quality multiple choice challenges
- 1 medium quality free text challenge

If you ask 1 medium quality multiple choice challenge, you must also ask at least one of the following:

- 5 low quality multiple choice challenges
- 3 low quality free text multiple choice challenges
- 1 low quality free text challenge and 3 low quality multiple choice challenges
- 2 low quality free text challenges and 1 low quality multiple choice challenges

If you ask 2 medium quality multiple choice challenges, you must also ask at least one of the following:

- 1 low quality free text challenge
- 1 medium quality multiple choice challenge

Score 3

The person will get a score of 3 if you do either of the following in person or remotely:

- make sure they physically match the photo on (or associated with) the strongest piece of genuine evidence you have of the claimed identity
- make sure their biometric information matches biometric information from the strongest piece of genuine evidence you have or an authoritative source of the claimed identity

Make sure someone matches a photo in person or remotely

The person doing the match must have all the skills and training needed to get a score of 2. They must refresh their training in how to detect impostors every year.

The person or system doing the match must do everything needed to check someone matches a photo (in person or remotely) at score 2. You must also make sure:

- your process has a way to identify if someone is wearing a mask, makeup or prosthetics to look like someone else
- their eyes are visible without any glare or reflections (if the person is wearing glasses)

Make sure someone matches biometric information

You must do everything needed to check someone matches biometric information at score 2. You must also make sure:

- the number of ‘false matches’ and ‘false non-matches’ (https://www.ncsc.gov.uk/collection/biometrics?curPage=/collection/biometrics/measuring-performance) in your system are appropriate for your security and usability needs and are based on industry best practice (for example ISO/IEC TR 29156:2015 (https://www.iso.org/standard/45235.html))
- your system uses a biometric algorithm that’s been proven to be effective against a recognised benchmark, like the National Institute of Standards and Technology’s (NIST’s) face recognition vendor test guidance (https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing)
- the person’s biometric information is captured under conditions that do not reduce the accuracy of the type of biometric check being used (things like light, noise, and humidity impact the success rates for different biometric modalities and should be adjusted if needed)
- your system can tell when someone is spoofing the system using an artefact that’s taken time, money and effort to create, for example detecting if someone is changing the pitch and adding background noise to a recording of a vocal biometric
- your system uses multiple processes or measures to confirm that the person is real (known as an ‘enhanced liveness’ test)

Example If you’re checking a facial biometric modality, you can ask the person to take a short video of themselves, during which they repeat a random sequence of words back to you. This helps you make sure there’s a real person involved. You can also continually assess small movements of the person’s head while the biometric measurement is taking place.

Score 4

The person will get a score of 4 if you make sure their biometric information matches biometric information from the strongest piece of genuine evidence you have or an authoritative source.

The system doing the match must do everything needed to check if someone matches biometric information at score 3.

It must also be able to tell when someone is spoofing the system using a sophisticated artefact that’s taken a lot of time, money, effort or criminal activity to create. If you’re checking a facial biometric modality, this could mean making sure the person is not showing a 3D animated avatar on a hijacked computer or device.

The biometric information on the evidence and the biometric information of the person must also be captured under ‘controlled conditions’. This means:

- any equipment has been designed in a way that makes it difficult to be tampered with
- someone who was trained in how to compare people to their identity evidence by a specialist trainer (such as the Home Office, National Document Fraud Unit or CPNI) supervises how the biometric information is captured
- the supervisor refreshes their training every year
- the supervisor monitors the behaviour of the person whose biometric information is being captured to make sure it’s not suspicious
- the area and equipment used to capture the biometric information has been designed in a way that reduces the likelihood of incorrect matches for the type of biometric information being used

Example Some facial recognition software will be less accurate in different light conditions. A facial biometric comparison should take place under the best light conditions for the biometric algorithm that's being used. This will reduce incorrect matches and false rejections.

The area where the check is being done should also be monitored by trained personnel who make sure people are not trying to fool the system.

Print this page