PRE-EMPLOYMENT SCREENING

DOCUMENT VERIFICATION

EDITION TWO: FEBRUARY 2015

© Crown Copyright 2015

We are grateful for the support and help provided by the National Document Fraud Unit in putting together this guidance. All images are owned and supplied by them.

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.
Introduction

Document verification is the process of ensuring that documents presented by prospective employees are genuine and that the holder is the rightful owner. It is an integral part of the pre-employment screening process. Staff responsible for checking documents should have the necessary knowledge and tools to be able to confirm authenticity and identify basic forgeries.

This document highlights the main security features present in a number of documents and the main methods used to forge such documents. It should assist staff in the detection of basic forgeries. However, this guidance will not provide staff with the skills to detect all forgeries, particularly those which have been produced using highly professional and sophisticated techniques. If you have concerns about a document you should always seek further advice (see page 34).

Most of the examples in this document relate to passports. However, some of the security features contained within passports are also in other documents, for example driving licences. The forgery techniques outlined in this chapter (e.g. chemical alteration), are relevant to all kinds of documents e.g. university certificates.

This document should be read in conjunction with ‘A Good Practice Guide on Pre-employment Screening’. This can be downloaded from www.cpni.gov.uk.

Document verification strategy

It is important that your document verification processes are integrated within your wider pre-employment screening strategy. This section sets out the key areas you will need to consider.

Application form

Information about the document verification process should be provided to all candidates as part of the recruitment process (in the application pack or on-line). This should clearly explain which documents are requested and why – for instance to guard against identity fraud and forgery. It is also worth stressing how important document verification is to your company and that you may seek to confirm the authenticity of relevant documentation. This may provide an element of deterrence to individuals who might apply using forged documentation. You may also wish to make it clear that applicants who are unable to produce the required documentation will not usually be employed (except for cases where a reasonable explanation can be provided).

Strategy checklist

- Make clear, as early as possible in the process, which documents are required.
- Emphasise the importance of document verification – this will help to act as a deterrent to would-be forgers and fraudsters.
Training

Consider the training needs of those staff responsible for document verification. How much knowledge do they already have? What sort of training might they require? How frequently should this be refreshed? You may wish to designate a particular member of staff as the internal ‘expert’ on document verification. They could be responsible for ensuring that all training needs are met and monitor developments in documents and detection techniques. They could also act as the first point of contact for staff who have concerns about any documentation.

You may decide to seek private sector training in document verification; there are a number of private sector organisations in the UK which offer such services. You could also develop your own internal training programmes. They may include the opportunity for staff to practice examining documents – such as their own passports – to ensure that your processes are practicable and understood. These sessions could also discuss any previous examples of document concern and how your staff dealt with the situation.

Document verification training checklist

Consider:

• The training needs of your staff.
• Appointing an ‘expert’ within the organisation responsible for all aspects of document verification.
• Whether your training needs can be met by private sector/external trainers.

Equipment

Consider whether your processes require the use of any verification tools. Both magnifiers and ultra violet (UV) light sources are easy to obtain and can enhance your ability to detect fraudulent documentation. However, the use of this equipment will only be effective if the users have a sound understanding of the document and its safeguards.

Magnifiers - Standard handheld magnifying glasses can be useful when examining documents for photo substitution (i.e. dirt around the photo, misalignment of safeguards which overlap from the page to the photo).

Ultra violet (UV) light sources - UV pens and UV light boxes are useful tools for identifying whether UV safeguards are genuine.

Document checking

The length of time required for examining documents is directly related to the skills of the staff responsible for checking documents. Consider the length of time needed to verify and photocopy documents and incorporate this into your recruitment process. For example, you may wish to do initial checks while the applicant is being interviewed, if that provides enough time.
It is essential that all documents are examined thoroughly. It may be helpful to design a checklist (such as the Document Verification Checklist at page 33) to ensure that all aspects of the document are examined. You could introduce procedures whereby each document will not be ‘signed off’ until each section of the checklist has been completed. Furthermore, it is important to conduct checks against every document that is presented.

**Document examination checklist**

- Consider how long your staff require to examine documents.
- Develop a checklist to ensure that all aspects of the document are examined.
- Examine all documents thoroughly.

**Concerns**

If you identify a potential concern with a document, you should first ensure that all other aspects of the document are checked before you take the matter further (this is when the use of a checklist may be helpful). You should then seek professional advice (see page 34) for contact details and help regarding travel documents. For other documents, you are advised to contact the originating organisation, for example the originating university for degree certificates.

Ideally, you should seek further advice before you return the document to the applicant. The advice you receive may be able to resolve the issue (for instance the apparent inconsistency was caused by wear and tear). If it is not possible to seek a second opinion, proceed with caution and raise your concern(s) with the applicant asking them whether they can provide an explanation. You should stress that you are following standard procedures for the verification of documents.

Photocopies of the relevant documents may be sufficient to conduct further investigation (e.g. concerns with the type face on the bio-data page of a passport). However, if your concerns lie elsewhere within the document you may have to ask the applicant to return with the original document which can then be examined by an expert or someone more experienced. Your concerns may relate to a document produced outside the UK, in which case it may be more difficult to resolve your suspicions. If your concerns relate to a passport or national identity card, the relevant embassy or consulate in the UK may be able to assist you.

If you are unable to resolve your concerns you may decide to discontinue the applicant’s recruitment. You should document all your dealings with the applicant (i.e. telephone calls, emails, letters etc.) and any other relevant parties. You may also wish to seek legal advice.

**Dealing with suspicious documents checklist**

- Complete your examination of the whole document before carrying out any investigations.
- Where necessary seek specialist advice.
- Raise any concerns with the applicant in a sensitive manner; there may be a plausible explanation.
- Consider discontinuing the applicant’s recruitment if you are unable to satisfy your concerns.
Security features

The examples of the security features in this section refer to the UK passport. However, these features are also present in a number of other documents such as the UK photo driving licence.

Documents often incorporate features that prevent the unlawful copying or alteration of the document. These security features are used in any document that has a value (such as identity documents, currency, driving licences etc.).

Substrate security features

A substrate is the material from which documents are made. Traditionally, the substrate in passports and identity cards has been paper, into which many features have been incorporated to protect the document against counterfeiting and forgery. However, an increasing number of nations are using a polycarbonate (hard plastic) substrate for the bio-data page. Security features contained within the substrate include:

Base fluorescence

Passports and identity cards are made from high quality security paper. This is designed to have a low base fluorescence (i.e. not react brightly) when exposed to ultra-violet (UV) light. Cheaper paper (frequently used by counterfeiters) tends to fluoresce to a greater extent under UV light.

Example of genuine (left) and counterfeit (right) under UV to show fluorescing of counterfeit paper. The counterfeit watermark also fluoresces under UV.

Watermarks

A watermark is created during manufacture by variations in the thickness of the paper and can be viewed using transmitted light (by holding the document up to light or passing light through the paper). A real watermark should consist of subtle changes in tone and both darker and lighter areas and should never react under UV light.
**Security fibres**

Security fibres appear in random patterns across the paper. They can be visible to the naked eye, or fluorescent when exposed to UV light.

.Security fibres under UV light source

**Security printing techniques**

The printing methods used in a number of documents can also contain a number of security features. These include:

**Intaglio printing**

Intaglio is a printing process which results in the ink having a raised and rough feel which can be felt by running a finger over the paper. Intaglio printing can be found on the inside cover of some (but not all) passports.

**Latent image**

This technique is applied using an intaglio process and the printing technique used means that the pattern can only be revealed by viewing the page at an oblique angle. The photo below shows both intaglio printing and the latent image on the inside of the front cover of the UK passport.

.Two photos of latent image within intaglio printing - the one on the left face on; to the right at an oblique angle displaying the latent image

**Gold blocking**

Gold blocking consists of a real gold leaf stamped hard into the cover of the passport. Genuine gold blocking will be of high quality and fine detail. When assessing gold blocking it is important to proceed with caution as the gold blocking in older passports can fade due to wear and tear.
Generally speaking, gold blocking in recently issued passports should be less faded. Potentially suspicious gold blocking is not conclusive. However, it should merit a closer look at the rest of the document.

**Laser perforations**

There are very fine laser perforations which can be seen by holding the bio-data page of the UK passport up to the light (photo on the following page):

![Holding UK passport up to transmitted light to accentuate the laser perforations around the corners of the photo](image)

**Diffractive optically variable imaging devices (DOVIDS) – holograms and kinegrams**

DOVIDs reveal an image or pattern when light is diffracted by the device. There are many different types of DOVIDs, the majority seen in passports are based on holographic technology (see the photo below).

**Lamination**

- **Standard laminate** – a sheet of clear plastic which can incorporate visible and invisible safeguards.
- **Laminates with Optically Variable Devices (OVDs)** – an example is the British passport where a clear plastic laminate featuring a transparent OVD protects the holder’s digital image.
OVD protecting digital image

**Basic photograph authentication**

This refers to any feature added at the time of issue, usually as a means of deterring the removal of the photograph of the holder. This may be an ink stamp (wet ink seal), or an embossed (dry seal) which can be linear or round.

1. Example of blue ink stamp over photo
2. Embossed dry seal

**Ultra-violet (UV) light**

Most passports and travel documents contain safeguards which can only be seen with UV light. Care should be taken because these safeguards can be simulated, but if they are completely missing it is likely that something is wrong with the document. Many passports include a UV safeguard which covers the holders photograph to protect against photo substitution. See below examples of UV safeguards in UK passports.
UK passport under UV light source highlighting crown on inside cover, stitching and flower edge

**Optical character recognition (OCR)**

A significant proportion of passports contain a series of machine readable characters on two rows along the length of the bio-data page of the passport. The font used for these characters is Optical Character Recognition (OCR B) (see below). This font has a number of distinct attributes. You can see that the number ‘three’ has a flat, as opposed to a curved, top line and the number ‘four’ has a broken vertical line. A check of these two digits on any passport should help to highlight any potential concerns.

**OCR B character set**

**Biometrics**

Biometric details enable an individual’s unique identity to be recorded. There are a number of physiological features that are unique to each individual which can be used to prove a person’s identity. Biometric identifiers include facial image, fingerprints or iris recognition. Although biometrics cannot completely protect documents against fraud, they help make passports harder to forge or counterfeit.

The UK has issued biometric passports (also known as ePassports) since 2006. The ePassport measures 125mm by 88mm, and complies with International Civil Aviation Organisation (ICAO)
standards and EU common format requirements. The standard issue passport contains 32 pages and the business passport 48 pages. The biometric passport will normally be valid for ten years. Passports issued to children under 16 are valid for five years.

The ICAO specified symbol on the front cover of the passport signifies that the passport contains a biometric chip, distinguishing the book from previous UK passports. The photographs overleaf show the new ‘e-logo’, printing design, UV features and biometric chip on the back of the bio-data page.

Example of UK biometric passport (also known as ePassport) first issued in 2006
Security features checklist

- High quality security paper should have low base fluorescence (i.e. should not react brightly) under UV light sources.
- Watermarks – viewed by passing light through the page; consisting of subtle changes in tones; watermarks should not react when placed under UV light sources.
- Latent image – a pattern or words revealed by viewing the page obliquely.
- Intaglio – printing process should be rough to the touch and contain a latent image revealed by viewing the page obliquely.
- Diffractive Optically Variable Imaging Devices (DOVIDs) – revealed when light is diffracted by the device i.e. holograms.
- Laminate – plastic layering on the document which can incorporate safeguards.
- Photo authentication – often a stamp overlapping the photo, designed to deter substitution.
- Safeguards which can only be seen when document placed under UV light sources.
- Biometrics – holder’s unique identity contained within the document, e.g. facial image or fingerprints.
Document fraud

Document fraud can be conducted in a number of different ways. This section aims to highlight how fraud takes place and how it can be detected. The majority of the examples of fraudulent documents relate to passport fraud and are therefore specific to photographic documentation.

The main types of fraud are:

- **Impostors** – the holder looks like the rightful owner.
- **Counterfeit** – made from scratch.
- **Forgery** - a genuine document which has been altered.

**Imposters**

This is the simplest type of document fraud, where the ‘holder’ is simply a look-alike and the document is often not altered at all. To guard against impostors you are advised to:

- Attempt to calculate the age of the person (using the date of birth in the document, if provided) and compare that with the person standing in front of you. It can be difficult to ascertain a person’s age from their appearance and is important to consider that people may have aged as much as ten years since their passport photo was taken. Therefore, you should proceed with caution.
- Compare the photograph in the document with the applicant – pay particular attention to the lips, chin, eyes, nose and if possible ears. This must be done in the presence of the applicant.
- Compare the signature in the document with one provided elsewhere by the candidate on their application form
- Compare as much of the data contained in the document with other information you have on the individual. For example, if the document is a degree certificate their education history on the application form should correspond.

**Counterfeits**

A counterfeit document is one that has been made up from scratch to resemble an officially issued document. The quality of counterfeits can vary enormously. While it may be very difficult to identify a high quality counterfeit the following information may help to identify counterfeits of lesser quality. It is not necessary to know what the original looks like since documents (particularly passports and visas) have many common safeguards built into them to make copying difficult.

**Watermarks**

By holding the document up to light you should be able to identify the watermark. A genuine watermark has subtle variations in the light and dark areas, unlike many counterfeit watermarks.
Example of fake (left) and genuine watermarks under transmitted light.

Following an examination of the document by transmitted light, you may want to study the document under ultra violet light. A genuine watermark should never react to ultra violet light, but a chemically simulated watermark is likely to fluoresce.

Example of genuine (right) and fake documents (on left that fluoresces) under UV light.

**Intaglio and latent image**

A relatively easy detection point for a counterfeit document may be the absence of intaglio print and a latent image which are often found on the inside cover of genuine travel documents. In a counterfeit the attempt to replicate intaglio may create a waxy feel unlike the rough surface of the genuine and may also lack detail.

Intaglio printing may also include a latent image. In a counterfeit document there may be no attempt to simulate the latent image. You can check this by holding the page where the latent image should be at an angle.
**Printing**

Genuine travel documents are manufactured on large scale security printing presses using high quality, solid colour print processes and are deliberately complex to make copying difficult. Counterfeits are often produced using colour copies or other scanning devices and this is likely to produce jagged edges compared to the solid lines of background print in a genuine document. Additionally, ink-jet printers cannot replicate the smooth transition between colours created by rainbow background print.

Example of two documents highlighting real (left) and fake (right) background printing

You can assess the quality of printing with the use of a magnifying glass – for instance the black print in a genuine visa is clear and even. The printing in a counterfeit document may lack intricate designs, without solid and clearly defined lines and shapes.

Spelling mistakes are also common as in the stamps below. The red squares highlight the mistakes, ‘CHANNEL TRAVEL’ should read ‘CHANNEL TUNNEL’ and ‘public ponds’ should read ‘public funds’.

Examples of stamps with spelling mistakes

**Gold blocking**

Gold blocking consists of real gold leaf stamped hard into the cover of the passport. Compare the quality and fine detail of the genuine with the counterfeit below:
Example of genuine (left) and fake gold blocking (right)

**Counterfeit checklist**

What to look for:

- Poor quality or misaligned gold blocking on the front cover of the document.
- Suspicious texture of cover, laminate or pages.
- Overall poor manufacture, i.e. misaligned covers.
- Missing, or simulated, intaglio.
- Sub-standard print quality.
- Absence of, or poor quality, UV safeguards.
- Absent or UV reactive watermark.
- Non-standard UV reaction of the paper.
- Poor quality photo authentication.

Use UV light in the detection of counterfeits to:

- Compare the overall fluorescence of a suspect document with a genuine one.
- Check for the presence or absence of UV safeguards.
- Check for a simulated watermark.

Note: some UV features may be diminished in worn but genuine documents.

**Forged documents**

A forged document is a genuine document which has been altered in some way to suit the new holder. Photos and personal details are obvious targets but pages, visas and stamps may also be forged. The main types of forgery are covered in this section.
Page substitution

A document will often be dismantled in order to substitute a page used to:

- remove an incriminating endorsement;
- benefit from a visa, stamp or residence permit; or
- change a photograph, image or personal details.

Covers and endpapers

To dismantle a passport one or both of the endpapers must be removed to access the reverse of the stitching. You should make allowances for wear and tear, but any localised damage or wrinkling to the endpapers or covers should be treated with suspicion.

Alignment

Pages are trimmed to a standard size and therefore should align exactly. In a forgery the pages may be misaligned due to the poor reassembly of the document. The pages of the booklet may not align with the spine and the endpaper may have separated from the soft cover.
Top image shows misaligned pages indicating poor assembly as does the image bottom right. Bottom left is a genuine document.

Page numbering

The International Civil Aviation Organisation (ICAO) recommends that passports contain a number unique to the document on every page. If genuine pages from other documents are substituted into a different passport then the number may be altered to match the new document. Close inspection of these unique numbers may highlight alterations.
Stitching

Passports which have been dismantled to remove the pages will often contain empty stitch holes where the original thread used to be. In addition the stitch holes of the page which has been inserted may not match those of the document again leaving vacant holes.

Example of tampered stitching

Note - Genuine pages from another document or part/completely counterfeit pages may be inserted into a passport. In modern passports, the most important page – the biographical data page – is most commonly substituted.

Page substitution checklist

How to tell if a page or pages have been substituted:

- Damage to the cover of the document.
- Damage to the spine of a document.
- Damage to the endpapers.
- Endpapers misaligned with the covers.
- Vacant or enlarged stitch holes.
- Loose stitching.
- Poor quality printing on a suspect page.
- Different, simulated or missing watermark.
- Inconsistent UV reaction of pages and safeguards.
- Incorrect number of pages.
Photograph substitution

Forgers involved in the photo-substitution of identity documents may decide to leave the details unchanged, resulting in a possible mismatch between the holder and the profile in the document. More commonly they may change the details to match the profile of the holder, risking detection if the alterations are too obvious. It is therefore always advisable to check the personal details (name, date of birth, height etc.) contained in an identity document against the person in front of you.

There are three main ways to substitute a photograph:

**Lifted laminate method**

An increasingly common method of forgery is a laminate lift which can result in few signs of damage to the document.

The main detection points for this style of forgery are:
• A second, counterfeit emboss or a misaligned emboss across the photograph and bio-data page.
• Damage or degradation to the laminate safeguards.
• Extraneous material beneath the laminate.
• Disturbed paper fibres or damage to the paper fibres beneath the laminate.
• Creases in the laminate, best seen with an oblique light source.

The window method

A window is cut in the laminate on the photograph page and the original photograph is removed. A new photograph is inserted and another laminate affixed over the page to conceal the damage.

If the laminate contains a visible safeguard the forger may decide to reapply only the part of the window containing the safeguard. This will result in damage to the safeguard. Evidence of such damage can include hand-drawn or misaligned parts of the ink stamp over the photograph area or embosses that are misaligned from the photo to the page. The obverse and reverse emboss impressions into the photo and page should also match. Counterfeit stamps and embosses may also lack fine detail.

Misaligned safeguards between photo and rest of page and showing signs of dirt
Split page method

The page containing the photograph is split along its edge or the photo page is split away from the cover. Once split the photograph can be accessed from behind. The main detection points for this style of forgery are:

- damage to the safeguards
- the cover may not be firmly affixed to its endpaper and the paper damage may be visible around the edge of the page or photograph.

Whichever photo substitution method is used, an unusually large photograph may be used to conceal any damage to the area where the original photograph was positioned.

Photograph substitution checklist

How to tell if a photograph has been substituted:

- An unusually large photograph.
- Misaligned dry seal (emboss) from photograph to page.
- Misaligned obverse and reverse impressions of the dry seal (emboss).
- Misaligned ink authenticating stamp from photograph to page.
- Ink stamp or authenticating signature continues beneath photograph.
- Poor quality ink stamp or dry seal (emboss) over photograph.
- Paper damage adjacent to or behind the photograph.
- Wrinkled or double laminate (latter may be evident by looking at the edge of the page).
- Air and dirt beneath the laminate.
- Excess glue around or behind the photograph.
- Inaccurate, broken or missing laminate pattern and/or UV safeguard.
- Page wrinkled behind or around photograph.
- Cut marks around the photo.

Use UV light in the detection of photograph substitution to:

- Check for unexplained patches of fluorescence behind or around the photograph, which may be indicative of excess glue or paper damage.
- Check for the presence, absence or inconsistency of UV safeguards in the laminate both over and adjacent to a photograph.

Digital Image substitution

Modern passports and identity cards are usually produced with the holder’s personal details digitally printed directly into the document and use digital images rather than photographs.

The main ways to substitute an image include:
Partial digital image substitution

When the actual face has been removed and the new holder’s face is inserted. For this technique the original hair and shoulders remain. On close inspection you may be able to see that the new face lacks the clarity of the shoulders and hair which are likely to be a higher resolution.

When cutting takes place to remove the image, cut marks in the page may become apparent when the page is viewed with the use of indirect light.

Whole digital image substitution

This involves the separation of page and laminate. A piece of paper containing the new image is grafted onto the page and the laminate then re-applied. This may result in localised damage to the bio-data page and to the visible laminate safeguard. The additional paper also adds thickness to the page and has a high base fluorescence when exposed to UV light.

Digital image substitution checklist

How to tell if a digital image has been substituted:

- Paper damage adjacent to or behind the image.
- Print damage adjacent to or behind the image.
- Wrinkled or double laminate.
- Air and dirt beneath the laminate.
- Ink run beneath the laminate.
- Inaccurate, broken or missing laminate pattern and/or safeguard.
- Unusual UV reaction in the image area.

Alterations

The following methods might be used to alter details within a document:

Mechanical (abrasion, rubbing, scraping of the paper surface)

If a document has been mechanically altered you may see:

- Under oblique light – raised fibres in the altered area.
- Under transmitted light – paper thinning in the altered area or thicker areas in the paper of the altered area (the forger may have added paper to cover up alteration, paper damage or used coloured correction fluid to conceal an alteration).

Chemical (liquids such as water, solvents, bleach)

When viewed under oblique or white light, you might expect to see shrinkage or wrinkling of the paper due to damage to print in the document if it has been chemically altered.
New details can sometimes be hand-written but are more often typed. The date of birth, height and gender should be checked carefully and you should look for smudging around the written details.

Bio-data which has been altered by scraping

**Alterations checklist**

- Is the page/document particularly wrinkled?
- Looking at the page at an angle are there any raised fibres?
- Are certain areas of the page thinner when the page is viewed with transmitted light?

**Stolen blanks**

A large number of genuine documents are stolen before they are issued and are subsequently used by fraudsters. To detect such documents it is important to check the authenticating stamps and overall quality of the type-written personal details carefully. If you have a known genuine passport from the same country you can compare the black print in-fill in both documents. You may find that the black print in-fill on the bio-data page is different in a stolen blank (see the examples below).

Genuine (left) and stolen blank (right) print in UK passports
**Visas**

Visas are secure documents in themselves and should have a similar standard of security as passports. However, visas are also open to fraud.

Substituted visas (those taken out of one document and, after alteration, inserted into another) may display signs of alteration to the passport number or personal and issue details.

Image substitution may also take place with visas. The use of transmitted light may reveal paper thinning caused by abrasion when the original image was removed. Further examination using UV light may show damage to the UV print safeguards which should be visible through the image.

If you have suspicions about the typeface you may wish to shine a powerful light through the page to test its thickness. The visa paper may well be thinner than the rest of the document due to the removal of the original typeface (through chemical treatment or scraping).

![Example visas](image)

**Examples of genuine visas**

**Visas checklist**

- Compare the biographical data in the visa with the same information in the passport and application form.
- Inspect the biographical data for signs of alteration.
- Check for smudging of the type-written details.
- Inspect the image on the visa for signs of substitution.
- Check for damage to UV safeguards.

**Alternative passports**

There have long been alternative travel documents which people have exploited when they have not wished to use a genuine passport using their true identity and nationality. There are other documents in circulation purporting to be valid for international travel but which are issued outside the accepted rules and procedures of international practice. Two of the main categories for this type of documents are:
Fantasy passports

These are documents with no authority and which are not officially recognised. They can occur in various forms and may have the physical appearance of a passport. They are not an acceptable statement of either nationality or identity.

Examples of fantasy documents

Camouflage passports

These are unofficial travel documents in the name of non-existent countries which are offered for sale by commercial organisations. The most recent examples to be issued are of countries which are no longer known by their original name, for example:

- Ceylon (Sri Lanka)
- Rhodesia (Zimbabwe)
- British Honduras (Belize)
- British Guiana (Guyana)

A person may buy a complete kit which can include birth certificate, driving licence etc.

Example of British Honduras kit
Other forms of identification

Identity cards and driving licences often contain some of the security features that are present in passports. The examples of the Polish ID card (below) demonstrate security features which include: lamination; high quality rainbow printing; a digital image and an optically variable device (OVD). Under UV examination further security features also become apparent.

Polish identification card under normal and UV light

The UK driving licence contains similar security features including high quality printing through a continuous background print and digital images. As the card is tilted an optically variable image (OVI) also appears. Under UV light, further security features can be seen.

Three different views of the same UK driving Licence highlighting background printing, OVI and UV safeguards

The UK driving licence counterpart document also has a number of security features including watermarks and UV features (see photos below). When presented with the counterpart check that the address is the same as provided on the application form and compare the signature. Look
closely at the printed details (including name and address) do these look faded, overwritten or modified in any way?

Three different views of the UK driving licence counterpart showing safeguards - the top without any light source inspection; the middle under transmitted light; the bottom under UV inspection

Other forms of identification checklist

- Compare the biographical data with the same information provided elsewhere by the applicant.
- Does the document have a laminate?
- Are there any optically variable devices?
- Check for UV safeguards.

Supporting documentation

These are documents which support an individual’s identity, proof of address etc. Examples of supporting documents include utility bills and mortgage statements. Supporting documents are not documents of identity.
Unlike identity documents, supporting documents do not have many security features. With the use of modern office equipment they can easily be forged, as the below example of a British Gas bill shows.

![British Gas bill – removal of correct address and new details added](image)

Despite the relative ease with which supporting documentation can be altered, close examination may help to identify inconsistencies or anomalies which warrant further investigation.

You should pay particular attention to the company’s logo on the bill. The British Gas example (below) shows how logos lose their quality when photocopied or scanned.
Top shows an original British Gas logo – middle laser printing, and bottom bubble jet printing

If you or your colleagues receive bills from the same company as the prospective employee, you may wish to make a comparison, focusing on the printing and quality of the paper.

The vast majority of bills are machine folded before being sent to customers. A bill which has not been folded should cause concern and be investigated further.

**Cheque books and bank cards**

These also include security features, including holographic images on credit/debit cards and high quality printing on cheque books. Check whether the handwriting or printing look faded or altered. Does the signature and handwriting look similar to other documents provided?

**Photo of bank card and cheque book under various light sources**

**Internet banking and bills**

An increasing number of people use the internet to bank and pay their bills. As a consequence many people no longer receive hard copy bills and an applicant may inform you that they are unable to provide a hard copy bill. They might offer, instead, to print a copy from their internet account. Such an approach is open to abuse and forgery. You should ask the applicant whether
they are able to provide a hard copy bill/statement. Alternatively, you can accept an internet bill or statement in conjunction with a separate, independently issued hard copy bill from another organisation.

**Recent change of address**

An applicant may be in the process of moving house. If this is the case, you should ask for the appropriate documentation from their previous address as it is likely that you will be checking that information also. You should always aim to satisfy yourself that all documentation is correct before recruiting an individual. However, in circumstances where the individual is unable to provide documentation to confirm their new address you should ask them to provide the appropriate documentation as soon as possible. If they are unable to do this you should ensure that you are satisfied with their reason.

Applicants may not be responsible for services (such as utilities) at their address (for example, an applicant who shares a property). However, this should not prevent the applicant from providing appropriate documents to confirm their residency, for example bank statements or documentation from their current employer.

If you have any concerns about supporting documentation, contact the individual. If you need to contact a utility company to confirm they provide a service to the given address, make sure you ask permission from the applicant first.

**Supporting documentation checklist**

- Compare the details in the document with the same information elsewhere e.g. addresses.
- Compare with known originals if possible – is the paper good quality?
- Is the logo well defined and clearly printed?
- Is the bill folded?
- If in doubt, discuss your concerns with the applicant and if required, with the service provider.

**Documents you should not accept**

You should not accept:

- Duplicate or photocopied identity documents (modern photocopiers often produce excellent results).
- An old-style provisional driving licence.
- An international driving licence (IDL) (easily and frequently forged). However, an international driving permit (IDP) is a genuine document purchased within the UK from the Post Office. It is an internationally-recognised additional document to support driving licences from any country.
- A copy of a birth certificate issued more than six weeks after birth (can be purchased on request for any individual without proof of identity).
- An old British visitor’s passport.
- Mobile telephone bills (as they can be sent to different addresses).
Basic document examination summary

The application of a few simple, non-destructive tests can identify the more obvious forgeries and counterfeits. Wherever possible, when examining documents compare them with known originals; if unsure seek a second opinion.

Check for impersonation (the simplest type of passport fraud)

- Carefully compare the photograph/image to the document holder.
- Check the age, visible marks and signature of the document holder. If practicable, ask the candidate to sign something in the presence of an authorised individual who can then compare the signature with that on the documentation provided.
- Check the chin, lips, ear shape (if possible), eyes and nose and their relation to the face as a whole.
- Check that the details given correspond with what is already known about the individual.

Check for evidence of counterfeiting

- Check the cover and overall construction of the document. Is the gold blocking well-defined and well-aligned? Do all the pages line up?
- Check the watermark. Use transmitted light first.
- Use ultra violet (UV) light. Does the watermark react (it shouldn’t)? What is the reaction of the paper? Are all the safeguards present?
- Check the print quality. If you are in any doubt as to what secure print should look like, have a look at a banknote.
- Are there any spelling mistakes?
- Is there any intaglio printing? Is it raised or rough when you touch it?
- Is it a fantasy document? Can you verify that the country or organisation exists?
- Take a note of the condition of documents in relation to issue dates.
- Check for incorrect issue dates (e.g. on public holidays or on the 31st of 30 day months).
- Compare the issue and expiry dates - the vast majority should correspond. Sometimes forgers only alter the expiry date.

Once you are satisfied that the document is not counterfeit, you can check for signs that the document may have been tampered with.

Checks for evidence of page substitution

- Do all of the pages align?
- Is the stitching correct?
- Do all pages react the same way when exposed to UV (they should in a genuine document)?
- Are all of the pages present?

Check for photograph substitution

- Check the authentication (e.g. wet ink stamp).
- Check that any safeguards in the laminate are present and undamaged (these may include UV reactive features).
• Check that there is only one laminate.
• Look for any cut marks around the photograph or, if there is one, along the lines of the photograph box.

Check for image substitution

• Look for any cut marks or paper damage around or behind the image.
• Check that any safeguards in the laminate are present and undamaged (these may include UV reactive features).
• Look for unusual UV reaction in the image area.

Check the stamps and visas in the document

• Visas are secure documents in themselves and should have security features to the same standards as passports.
**Document verification checklist**

Note: you should only use this checklist after having read and gained an understanding of this document.

<table>
<thead>
<tr>
<th>Question</th>
<th>Cause for concern</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Condition</strong></td>
<td></td>
</tr>
<tr>
<td>How does the age of the document compare with the issue date?</td>
<td></td>
</tr>
<tr>
<td>Do all the pages line up when closed?</td>
<td></td>
</tr>
<tr>
<td>Is each page numbered?</td>
<td></td>
</tr>
<tr>
<td>Are any of the stitching holes enlarged or empty?</td>
<td></td>
</tr>
<tr>
<td>Are there any red fibres around the type face?</td>
<td></td>
</tr>
<tr>
<td><strong>Photo (if applicable)</strong></td>
<td></td>
</tr>
<tr>
<td>Compare the document’s photo with the applicant</td>
<td></td>
</tr>
<tr>
<td>Is there a difference between the face and the shoulders?</td>
<td></td>
</tr>
<tr>
<td>Are there any visible safeguards over the photo? Do they match up between the photo and the page?</td>
<td></td>
</tr>
<tr>
<td>Is there an edge, cut marks or ridge between the photo and page (run your finger across the page)?</td>
<td></td>
</tr>
<tr>
<td>Is the photo area noticeably thicker than the rest of the page?</td>
<td></td>
</tr>
<tr>
<td>Is there any dirt around the edge of the photo?</td>
<td></td>
</tr>
<tr>
<td>Is there only one laminate (view at the edge of the page)?</td>
<td></td>
</tr>
<tr>
<td><strong>Biographical data</strong></td>
<td></td>
</tr>
<tr>
<td>Compare the bio-data (date of birth, signature etc.) with the same information provided elsewhere by the applicant.</td>
<td></td>
</tr>
<tr>
<td>Check for spelling mistakes including visas and stamps.</td>
<td></td>
</tr>
<tr>
<td><strong>Examination under natural/lamp light</strong></td>
<td></td>
</tr>
<tr>
<td>Can you see a watermark? (Genuine watermarks have subtle changes of tone and both darker and lighter areas)</td>
<td></td>
</tr>
<tr>
<td><strong>Examination under ultra-violet light</strong></td>
<td></td>
</tr>
<tr>
<td>Does the watermark react under UV? Watermarks should never react under UV.</td>
<td></td>
</tr>
<tr>
<td>Does the page react under UV? Genuine pages should only have a low base-fluorescence (i.e. should not react brightly).</td>
<td></td>
</tr>
<tr>
<td>Are there any patches of fluorescence around the photo? This could indicate photo substitution.</td>
<td></td>
</tr>
<tr>
<td>Is there a UV safeguard that runs over the photo? If not, this could indicate photo substitution.</td>
<td></td>
</tr>
<tr>
<td><strong>Printing</strong></td>
<td></td>
</tr>
<tr>
<td>Is the printing on the inside front cover raised and rough (run your finger across the page)?</td>
<td></td>
</tr>
</tbody>
</table>
Where to get help

CPNI offers free training to organisations in the critical national infrastructure on identity and document verification. For further details, please contact your CPNI adviser.

If you have concerns about the validity of documents presented to you, you should contact the UK Visas and Immigration (UKVI) Employers’ Helpline on 0300 123 4699. They will treat any information you provide in confidence and pass this on to the relevant UKVI Local Enforcement Office for further investigation. Often there may be criminal offences other than production of a forged document involved. If you suspect that this is the case, you should contact your local Police, who in turn will contact the local Enforcement Office.

If it is a foreign document, then the relevant embassy may be able to assist you. Alternatively, you may find useful information in government owned or sponsored websites.

Operation Fairway

The purpose of Operation Fairway is to detect, deter, and disrupt terrorist attack planning in the UK. It is managed and coordinated by the Metropolitan Police Counter Terrorism Command.

Operation Trammel (a strand of Operation Fairway) was launched in April 2003. Its aims include: to identify individuals who use fraudulent or fraudulently obtained genuine travel, and identity documentation to support international terrorist activities.

Of current concern is the misuse of forged or stolen passports or other identity documents to gain employment in vulnerable premises.

Do you know who you are employing?

The Fairway Team offers free Document Awareness workshops to HR and recruitment departments of companies vulnerable to terrorist attack, and aims to increase their knowledge of identity documents and the potential for their abuse.

For Operation Trammel enquiries or to find out more about Fairway document awareness, please contact nactso@cpni.gsi.gov.uk or telephone 020 7084 8433.