Tackling Hiring Fraud

The UK’s Response to a Growing Problem

In collaboration with:

Reed Screening

BHI
Better Hiring Institute

cifas
Fighting Financial Crime Together

S T Smith
Safeguarding Consultants Ltd

Foreword

Simon Fell MP
Barrow and Furness

Fraud is at epidemic levels in the UK. And it is becoming increasingly more organised and sophisticated. The picture is no different amongst organisations involved in recruitment.

Case studies clearly show that hiring fraud is typified by organised attempts to infiltrate organisations, and to target work seekers as they attempt to find work. This type of fraud causes terrible impacts on society: organisations going bankrupt at the hands of bad actors resulting in layoffs and redundancies; tragic safeguarding issues caused by those intent on fooling the system, and financial and personal detail loss for the public in the process of looking for work.

As the Prime Minister's Anti-Fraud Champion I am delighted to support this comprehensive guide for all UK employers on how they can prevent hiring fraud, both against themselves, and within their supply chains. Supporting industry to fight back against fraud is an important part of our overall fraud prevention strategy, ultimately with the aim of protecting citizens and businesses across the UK.

The work of the Better Hiring Institute to make UK hiring faster, fairer, and safer is critical to how we drive future competitiveness and prosperity. This guide represents a UK first, a critical part of how we make UK hiring safer for all, especially during this period of great technological change.

Simon Fell

Introductions

James Morris MP

Halesowen and Rowley Regis

Making UK Hiring the fastest globally is critical to our aims of growing the economy, improving productivity, and cutting waiting lists and workloads. In making UK Hiring the fastest globally and employing the latest technology, the risks of fraud and discrimination increase. Therefore it is essential that as we make UK Hiring faster, it must also be fairer and safer. This first of its kind guidance for UK employers is designed to help make UK Hiring the safest it can be. This will help tackle illegal working, prevent UK business from losing hard-earned income to fraudsters, often based overseas, and protect jobs and the economy.

I am delighted to provide the introduction to such an important piece of work, the first to ever tackle the entire spectrum of Hiring Fraud targeting UK business. By providing expert advice to UK business we can work together to drive future prosperity and tackle fraud. The guide is also designed to help work seekers and flexible workers in the supply chain to ensure we tackle the growing challenge posed by employment scams and unscrupulous intermediaries targeting people in need of work.

With industry and government working together we can reduce fraud, protect jobs, grow the economy, and help to tackle productivity and waiting list challenges. I hope industry uses this guide in the way that is most beneficial to them and through this work we help UK businesses and work seekers across the country.

Keith Rosser

Director of Reed Screening
Chair of the Better Hiring Institute

This is a really important piece of work. The Better Hiring Institute are revolutionising UK Hiring, creating the first national frameworks for hiring which, in turn, is enabling the creation of "Better Hiring Toolkits" at an industry level, toolkits that cover 80% of the UK workforce. The purpose is to make UK Hiring the fastest globally, the fairest in the world, and the safest it can be. Working with over 10,000 employers and UK Government it became clear that the biggest growing threat to hiring is from hiring fraud. It is becoming more widespread, more organised, and more harmful.

Launching this work in Parliament with MPs, Peers, industry, and all with the support of the Prime Minister's Anti-Fraud Champion, spoke volumes for the scale and sophistication of hiring fraud: including the rise of Reference Houses, deepfakes, abuse of artificial intelligence, and the evolution of fake identities and false documents.

Making hiring safer for business and for work seekers is essential if we are to grow the economy and protect UK companies and jobs.

This guide outlines the practical steps companies can take to drive out fraud and bad practice. It is meant to be an evolving guide as new threats and solutions are identified. The Better Hiring Institute offers a range of free guidance, advice, and help whilst campaigning to make UK Hiring faster, fairer, and safer. If your company is not already involved, join today for free via the website and become part of the biggest ever reform movement of UK Hiring.

Mike Haley

CEO of Cifas

The world of work has changed considerably over the last few years, with many organisations shifting away from traditional office working to a more flexible, hybrid pattern of working. Unsurprisingly, this has opened up fresh opportunities for fraudsters to target organisations, as well as employees to commit fraud.

Over the last couple of years, we have seen a rise in job seekers exaggerating and falsifying their experience and qualifications when applying for positions. As a result, there has been a sharp increase in cases filed to the Cifas Insider Threat Database, with around a quarter of these relating to the concealment of employment history.

The rise in recruitment fraud has also been fuelled by the growth of 'Reference Houses' to provide 'crash courses' in certain skill sets, as well as supply fake employment references and documents. These are now so sophisticated that it is getting increasingly difficult for recruiters to spot them during the pre-employment screening process.

In addition, the cost-of-living crisis has also meant that recruiters have also had to be vigilant to employees being targeted by organised crime gangs to provide personal data about their customers or their employer in exchange for cash.

Recruitment fraud is now widespread and far-reaching. Most organisations will be acutely aware of the serious consequences of a fraudulent hire, including data theft, financial losses, reputational damage, and regulatory penalties.

I am delighted to support the work of the Better Hiring Institute in raising awareness of the potential impact of recruitment fraud as well as helping UK businesses better understand how they can protect themselves.

Fraud cannot be fought in isolation, and so it is crucial that we continue to work together to combat this growing threat.

About this Guide

This is the UK's first comprehensive guide for organisations on how to tackle Hiring Fraud.

The guide will detail the most common types of fraud used within hiring and will give practical examples on how to prevent it.

What is...

Hiring Fraud?

Hiring Fraud encompasses any fraud committed during the hiring process. This may be committed by an individual against an organisation, or committed by an entity against a work seeker.

What are the consequences of fraud?

The consequences of fraud to your organisation can be both financially and reputationally damaging. The type of fraud that is being committed is ever evolving and organisations are investing more into their internal processes to combat this.

The case study below shows how easily an individual and organisation can be the real life subject of fraud and what the consequences could be:

Case study

An individual was approached in a coffee shop and offered the opportunity to be provided with a falsified employment history, along with a crash course in a specific process which would allow them to gain employment. After being turned down for multiple jobs due to lack of experience, the individual decided to pay the £500 that was being asked for this service. After their 2-week training course and with the use of a falsified reference they were offered a role. The individual was later approached by the group who supplied the falsified reference, and training and told that if they did not facilitate fraudulent transactions for them then they would tell their employer that they had obtained the job dishonestly. They started committing facilitating fraudulent transactions which were in the region of £500,000 and were arrested when the transactions were identified.

How can I use this guide?

The guide is divided into clear sections which are based on the most commonly targeted areas of fraud. The type of fraud included could occur through one of the following means:

- Fraudulent activity by an individual applying to work for you.
- An act carried out by a member of your current workforce.
- An example of where your organisation name and reputation are used during the hiring process in a fraudulent manner for the benefit of others.

Each example will include a brief description of what the type of fraud is, will give real life case studies or scenarios of how this might occur, and what you can do to protect your organisation and your workers to prevent it happening.

For ease, click on the relevant link to take you to that specific section:

1. Reference fraud
Includes fake references & Reference Houses

2. Qualification fraud

3. Fake application documents

4. CV based fraud
Includes falsified employment history & fake work history

5. Employment scams
Includes fake job adverts & social media messaging scams

6. Manipulation of artificial intelligence
Includes deep fakes & virtual interviewing

7. Dual employment

8. Immigration fraud

9. Fraud as a result of recruitment agency usage, including:
   a. Worker impersonation
   b. The use of non-compliant agencies

How can I protect my organisation?

We have put together a checklist of key actions you can take to minimise the likelihood of fraudulent activity having a significant impact on your organisation. These are linked to the fraud areas detailed in the "How can I use this guide" section.

Action	What will this help to prevent?
If outsourcing pre-employment screening, ensure you pick a reputable provider who has systemised fraud detection checks, utilising the latest innovation.	✓ All types of fraud
Utilise fraud prevention databases and working groups (for example, Cifas or the Better Hiring Institute sub-committees) to work collaboratively with colleagues across industry.	
Encourage a culture of curiosity, encouraging and enabling employees to challenge suspected fraud.	
Train your hiring team on the threats of Hiring Fraud and the common tell-tale signs of each fraud type throughout the guidance.	
Address the issues of those being scammed by fakes, creating best practice guidance and ensuring that reporting lines to JobsAware and Action Fraud are clear.	
Ensure that your onboarding technology is current, with the ability to enable IP address look ups and AI checking and detection software.	✓ Fake references & 'Reference Houses' ✓ Qualification fraud ✓ Fake application documents ✓ CV based fraud ✓ Dual employment ✓ Manipulation of Artificial Intelligence
Obtain independent verification of employment and activity history through third party government and other authoritative sources like open banking, payroll data or HMRC lookups.	✓ Fake references & 'Reference Houses' ✓ Qualification fraud ✓ Fake application documents ✓ CV based fraud ✓ Dual employment
Utilise the BHI Best Practice Guide on identifying fake references and identifying name changing in hiring.	✓ Fake references & 'Reference Houses' ✓ Qualification fraud ✓ Fake application documents
Consider using digital right to work checks, when appropriate, to prevent illegal working.	✓ Fake references & 'Reference Houses' ✓ Immigration fraud
Conduct overemployment monitoring checks when hiring and periodically throughout employment.	✓ Dual employment
When utilising a job board for advertising your vacancies, ensure they can evidence compliance with the Online Safety Act through third party accreditation.	✓ Employment scams
Use reputable recruitment agencies when outsourcing your hiring needs who are compliant with UK law and hold the necessary licences and accreditations.	✓ Fraud as a result of recruitment agency usage

Spotlight on Hiring Fraud

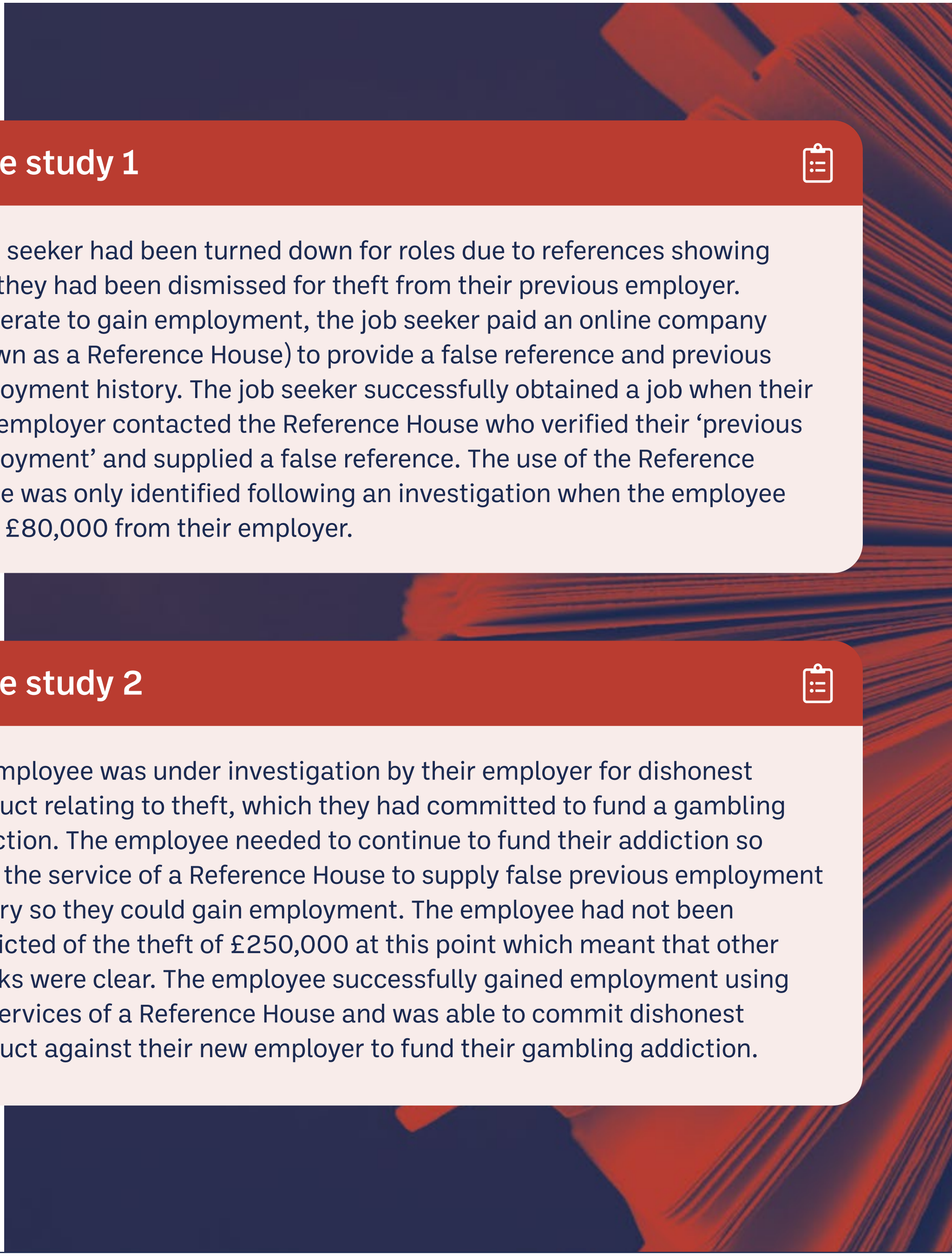
Reference fraud

Includes fake references & Reference Houses

A ‘Reference House’ is a term that has been defined to represent fraudulent organisations providing a fake reference for an individual at a cost.

The telephone number/email address that the individual provides for the referee will in fact be the details of the Reference House and they will subsequently provide the fake reference. Often, the contact details are very similar to a legitimate company and some Reference Houses even go as far as creating their own legitimate website and offering services such as fake bank statements for the individual to use to support the reference if challenged.

It allows an individual to create a fictious job in a legitimate company in order to give the impression that they are a qualified, experienced worker. This could be utilised in order to cover a lack of experience, full employment history or at worse, a period of time spent incarcerated. This could also be used for an individual to be able to pass the vetting checks of an organisation in order to gain access with the purpose of gaining data or defrauding the organisation themselves.



Case study 1

A job seeker had been turned down for roles due to references showing that they had been dismissed for theft from their previous employer. Desperate to gain employment, the job seeker paid an online company (known as a Reference House) to provide a false reference and previous employment history. The job seeker successfully obtained a job when their new employer contacted the Reference House who verified their ‘previous employment’ and supplied a false reference. The use of the Reference House was only identified following an investigation when the employee stole £80,000 from their employer.

Case study 2

An employee was under investigation by their employer for dishonest conduct relating to theft, which they had committed to fund a gambling addiction. The employee needed to continue to fund their addiction so used the service of a Reference House to supply false previous employment history so they could gain employment. The employee had not been convicted of the theft of £250,000 at this point which meant that other checks were clear. The employee successfully gained employment using the services of a Reference House and was able to commit dishonest conduct against their new employer to fund their gambling addiction.

Reference fraud: **What can I do to prevent it?**

When onboarding new workers, it is imperative to be vigilant and question anomalies. This could include:

- Does the email address look official and are there any spelling errors/additional characters added?
- Does the dates of the reference match the employment history shown on the CV?
- Does the referee's job title suggest a position of responsibility?

If using the services of an outsourced screening provider, they should offer solutions via the use of technology to do the following:

- Utilise a pre-verified employer/referee database to ensure the legitimacy of references, flagging suspected fraudulent reference providers.
- Obtain independent verification of employment and activity history through third party government and other authoritative sources like open banking, payroll data or HMRC lookups.
- Utilise integration with Companies House to check that the company being used for the reference exists (which would be corroborated with website checks).
- System based intervention to flag references which could be cause for concern for further verification.
- Use a referencing system that can support IP address lookup; exploring pattens in the references to identify fraudulent trends.

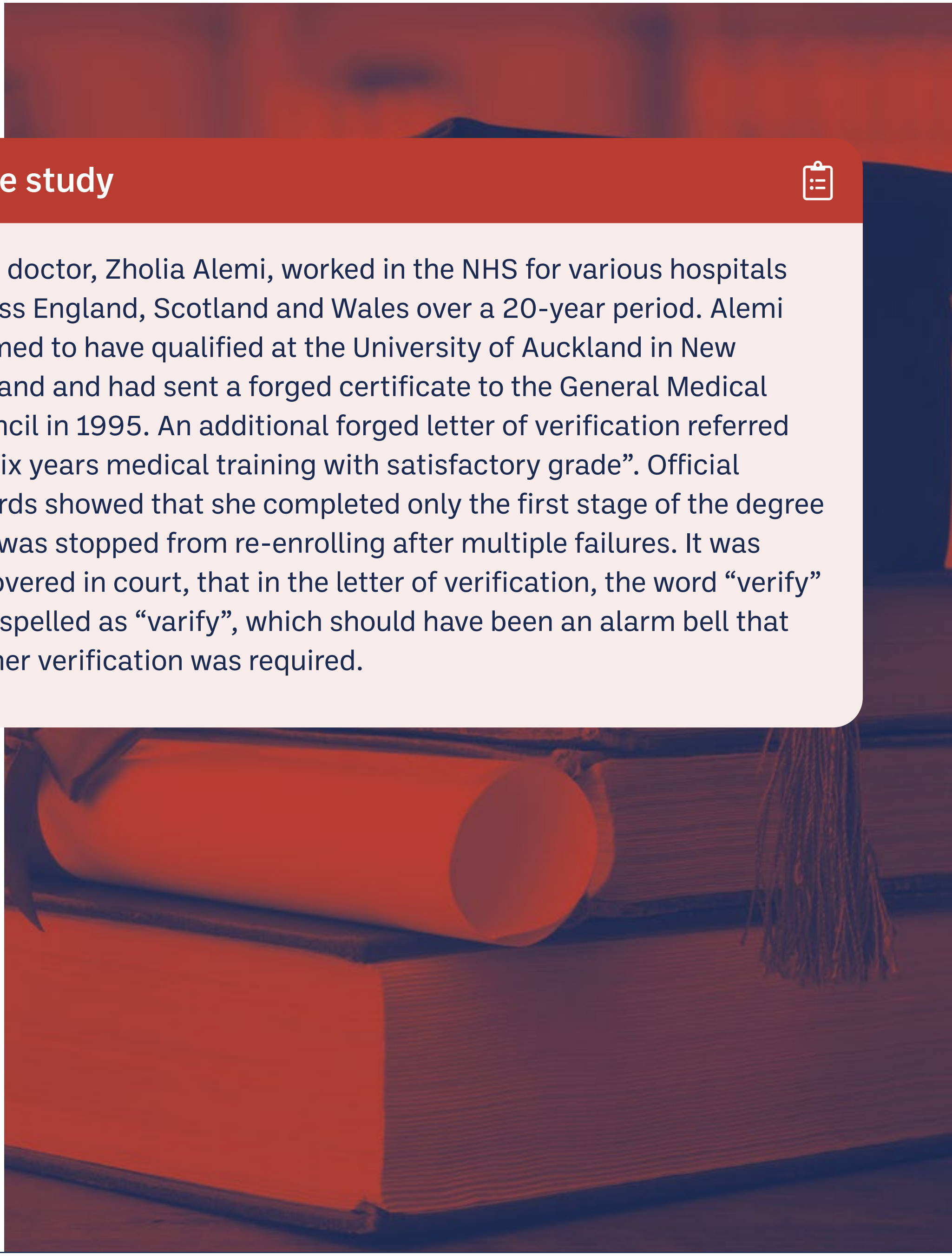
Utilise fraud prevention databases and working groups (for example, Cifas or the Better Hiring Institute sub-committees) to work collaboratively with colleagues across industry, focused on information sharing to discuss telltale signs and best practice tips.

Qualification fraud

Qualification fraud is the act of using fake or forged qualifications to gain an advantage in education or employment. It can take various forms, such as:

- Creating or buying counterfeit degree certificates from degree mills, so called 'novelty certificate' websites and fake or unaccredited universities.
- Lying about or exaggerating academic achievements or credentials on a CV or application form.

It will usually occur as a result of an individual not holding the relevant certifications that are mandatory for a job role. Some organisations will also require a set grade/level to be obtained by applicants and so individuals may also be tempted to alter such details to meet requirements/criteria.



Case study

Fake doctor, Zholia Alemi, worked in the NHS for various hospitals across England, Scotland and Wales over a 20-year period. Alemi claimed to have qualified at the University of Auckland in New Zealand and had sent a forged certificate to the General Medical Council in 1995. An additional forged letter of verification referred to "six years medical training with satisfactory grade". Official records showed that she completed only the first stage of the degree and was stopped from re-enrolling after multiple failures. It was uncovered in court, that in the letter of verification, the word "verify" was spelled as "varify", which should have been an alarm bell that further verification was required.

Qualification fraud: **What can I do to prevent it?**

When checking documentation as part of the application process, there are telltale signs to look out for to confirm if the document is not genuine:

- An incorrect or false awarding organisation name.
- Spelling errors or poor grammar.
- Incorrect qualification title.
- Poor quality of the document.

To go one step further, the following can be used to check authenticity of certificates:

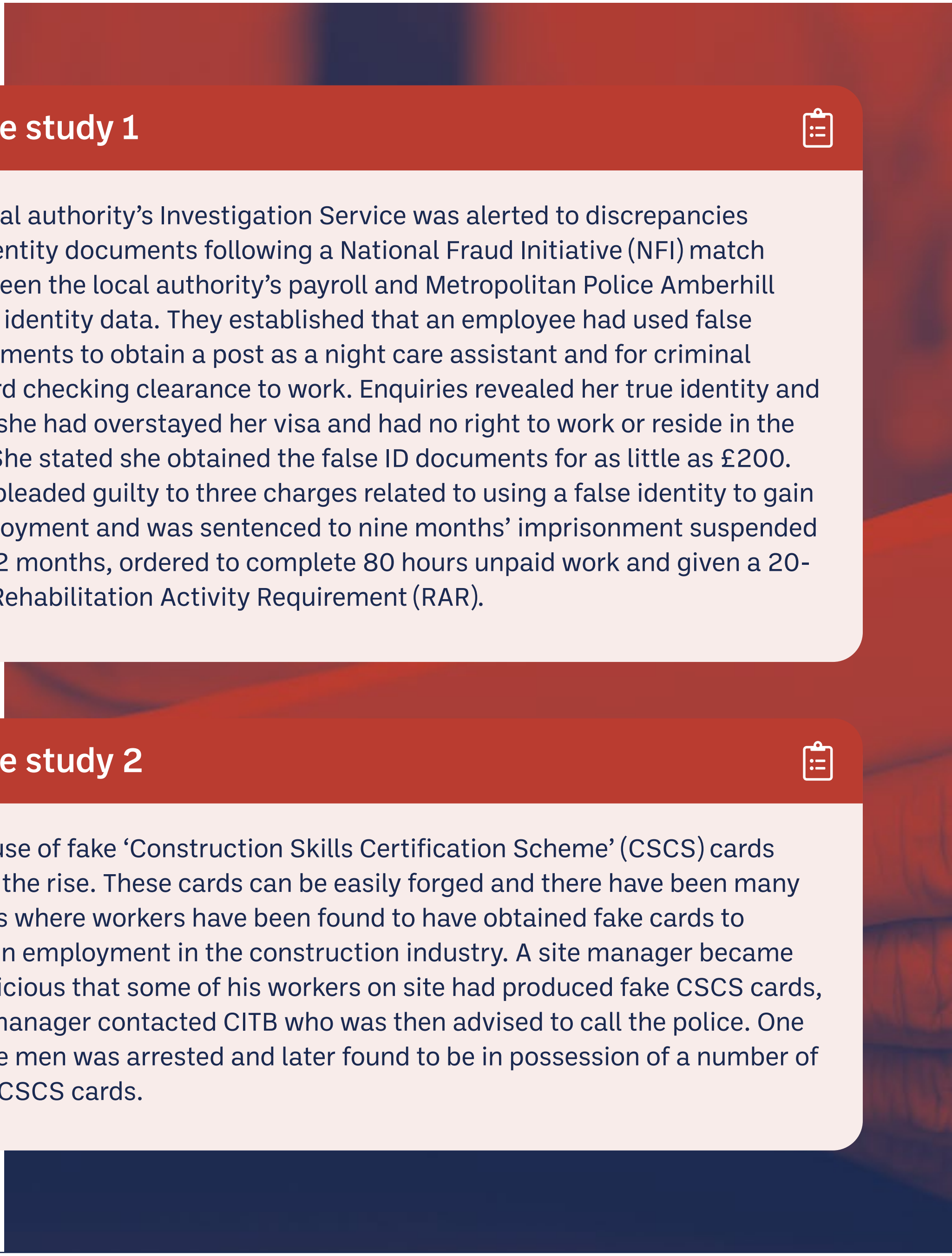
- Consider outsourcing to employment screening specialists who will be aware of the common signs of fraud.
- Contacting the organisation that issued the certificate to confirm that the individual did complete the course.
- Utilise machine learning including AI based document fraud analysis to review documentation provided as evidence by either the candidate or third parties to ensure absolute legitimacy.
- Conduct checks on verifying the authenticity of higher education qualifications. Please note that there are charges associated with these checks: High Education Degree Datacheck (HEDD) | Appruvr
- Train your hiring team on how to check the authenticity of certifications, for instance being able to spot common red flags.

Fake application documents

Similar to qualification fraud, the use of fake application documents can be used to gain an advantage in employment. It can take various forms, such as:

- Creating or buying counterfeit professional registration from fake websites and fraudsters for fees as little as £50.
- Obtaining fake proof of identity and address documents.
- Creating fake documentation to bypass industry specific checks and standards.

It will usually occur as a result of an individual not holding the relevant documentation that is required for a certain role. Some organisations will have a minimum level of checks in place in order to apply and subsequently be successful in a role and so individuals may be tempted to alter such details to meet requirements/criteria.



Case study 1

A local authority's Investigation Service was alerted to discrepancies in identity documents following a National Fraud Initiative (NFI) match between the local authority's payroll and Metropolitan Police Amberhill false identity data. They established that an employee had used false documents to obtain a post as a night care assistant and for criminal record checking clearance to work. Enquiries revealed her true identity and that she had overstayed her visa and had no right to work or reside in the UK. She stated she obtained the false ID documents for as little as £200. She pleaded guilty to three charges related to using a false identity to gain employment and was sentenced to nine months' imprisonment suspended for 12 months, ordered to complete 80 hours unpaid work and given a 20-day Rehabilitation Activity Requirement (RAR).

Case study 2

The use of fake 'Construction Skills Certification Scheme' (CSCS) cards is on the rise. These cards can be easily forged and there have been many cases where workers have been found to have obtained fake cards to obtain employment in the construction industry. A site manager became suspicious that some of his workers on site had produced fake CSCS cards, the manager contacted CITB who was then advised to call the police. One of the men was arrested and later found to be in possession of a number of fake CSCS cards.

Fake application documents: **What can I do to prevent it?**

When checking documentation as part of the application process, there are telltale signs to look out for to confirm if the document is not genuine:

- An incorrect or false issuing organisation name.
- Spelling errors or poor grammar.
- Incorrect qualification title.
- Poor quality of the document.

To go one step further, the following can be used to check authenticity of certificates:

- Consider outsourcing to employment screening specialists who will be aware of the common signs of fraud.
- Utilise machine learning including AI based document fraud analysis to review documentation provided as evidence by either the candidate or third parties to ensure absolute legitimacy.
- Train your hiring team on how to check the authenticity of certifications, for instance being able to spot common red flags.

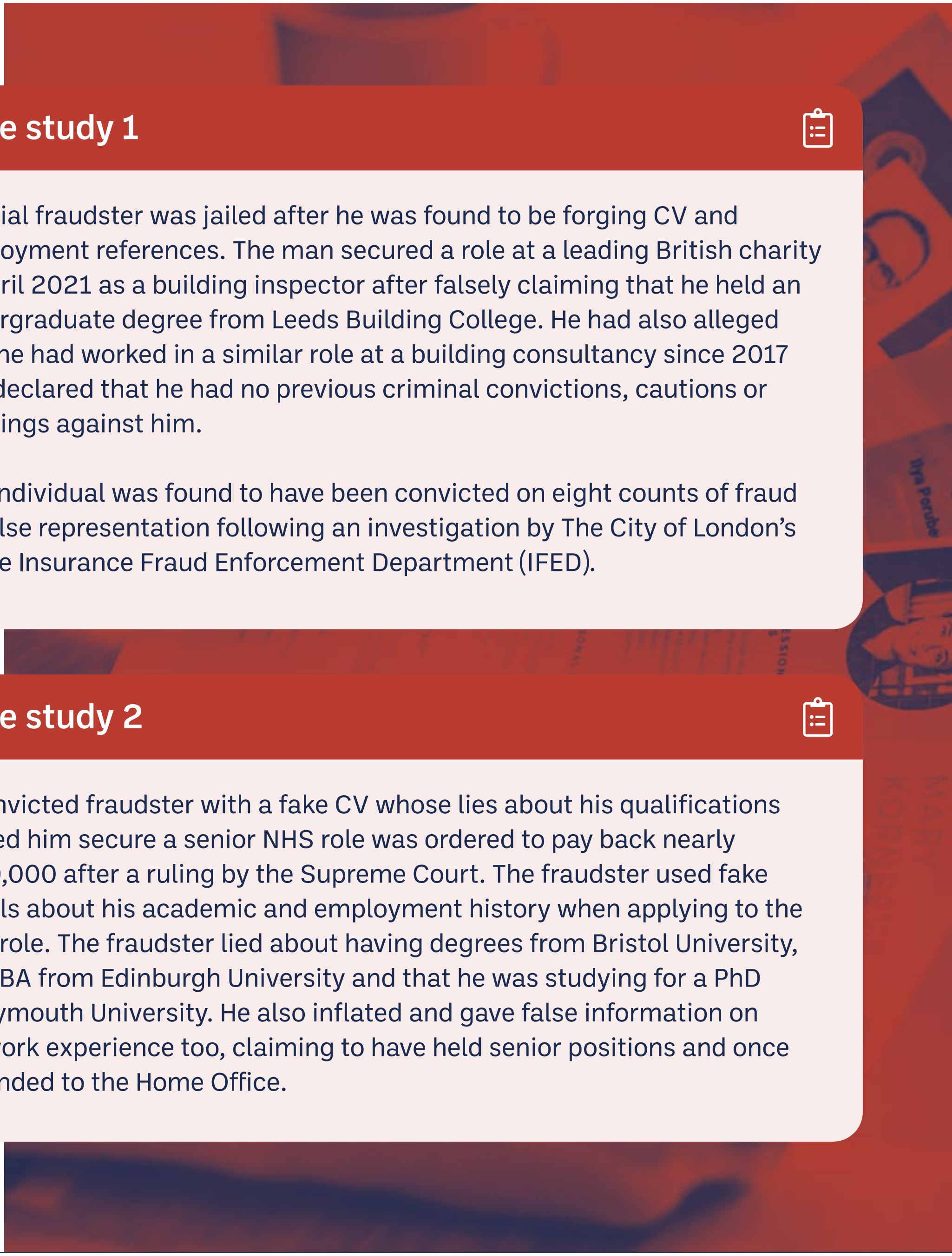
CV based fraud

Includes falsified employment history & fake work history

False employment or CV based fraud encompasses the act whereby an individual will insert false details of their employment which deliberately intends to mislead a person or organisation. False details on a CV can include posts undertaken, misrepresenting employment dates and tenure, qualifications/accreditation awarded, concealment of employment gaps and false claims of achievements, awards, or recognitions.

This could be done for the following reasons:

- Making the work seeker seem more qualified/experienced than they actually are by inflating the roles/responsibilities in previous employment/education.
- Hiding a period of unemployment which may make them more undesirable as an applicant or will mean that they may not meet the vetting criteria.
- Concealing a period spent of time spent in prison.
- Exaggerating salary levels.



Case study 1

A serial fraudster was jailed after he was found to be forging CV and employment references. The man secured a role at a leading British charity in April 2021 as a building inspector after falsely claiming that he held an undergraduate degree from Leeds Building College. He had also alleged that he had worked in a similar role at a building consultancy since 2017 and declared that he had no previous criminal convictions, cautions or warnings against him.

The individual was found to have been convicted on eight counts of fraud by false representation following an investigation by The City of London's Police Insurance Fraud Enforcement Department (IFED).

Case study 2

A convicted fraudster with a fake CV whose lies about his qualifications helped him secure a senior NHS role was ordered to pay back nearly £100,000 after a ruling by the Supreme Court. The fraudster used fake details about his academic and employment history when applying to the NHS role. The fraudster lied about having degrees from Bristol University, an MBA from Edinburgh University and that he was studying for a PhD at Plymouth University. He also inflated and gave false information on his work experience too, claiming to have held senior positions and once seconded to the Home Office.

CV based fraud: **What can I do to prevent it?**

To prevent employing a fraudster it is crucial to keep an eye out for the following elements in a CV/ employment history:

- Lack of detail or specificity.
- Gaps in employment history or missing references.
- Claims that cannot be verified or checked.
- Irregular formatting or poor grammar.
- Inflated job titles and responsibilities.

To go one step further, you can verify a CV is genuine is by:

- Utilising services to independently verify employment and activity history through third party government sources and other authoritative sources like open banking, payroll data or HMRC Gateway data (which instantly verifies employment claims on CVs).
- Verifying educational and professional qualifications. See the ‘Qualification Fraud’ section for best practice tips on how to do this.
- Asking the individual to provide evidence of achievements, awards or recognitions.
- Train your hiring team on how to check the authenticity of certifications, for instance being able to spot common red flags. Some employment screening companies work 24/7 in the UK to help support UK businesses to conduct these checks.
- Encouraging employees to report suspected CV fraud.

Employment scams

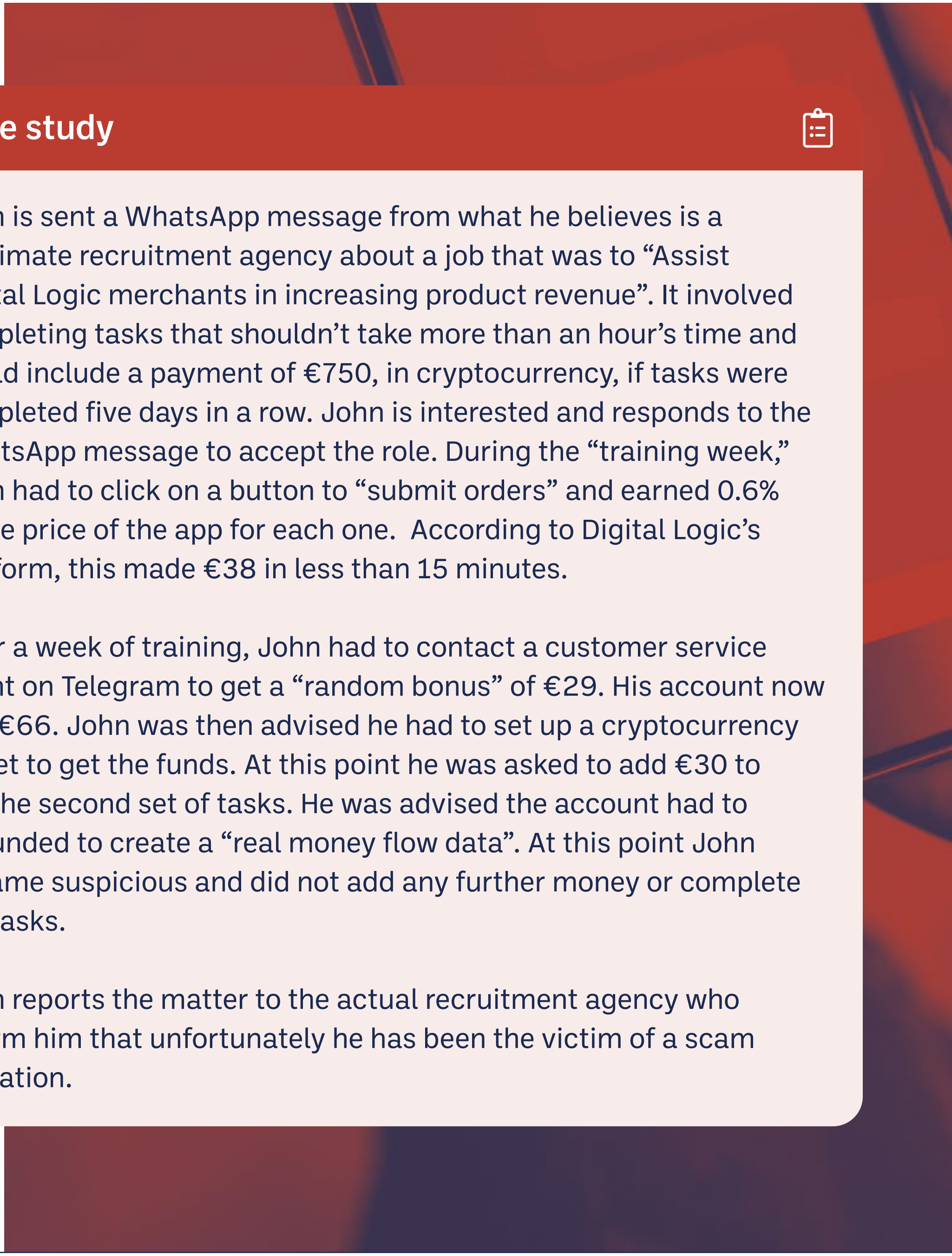
Includes fake job adverts & social media messaging SMS scams

Employment scams, involving messaging platforms, typically involve a scammer impersonating either a recruitment agency or legitimate organisation, and luring victims in with promises of work that don’t exist.

The ‘recruiters’ offer flexible working hours and working from home with a tempting pay offer, which will usually be in cryptocurrency. Once the individual is engaged, the scammer will seek ways to obtain money from them, often by making them pay upfront for training or equipment that is required for the job.

This scam has also been used to obtain personal data from individuals who believe they are providing identity documentation and other information for the purpose of vetting checks for their new role.

It is important that your organisation is aware of this as scammers may be using your company name and similar contact details as the basis of their scam.



Case study

John is sent a WhatsApp message from what he believes is a legitimate recruitment agency about a job that was to “Assist Digital Logic merchants in increasing product revenue”. It involved completing tasks that shouldn’t take more than an hour’s time and would include a payment of €750, in cryptocurrency, if tasks were completed five days in a row. John is interested and responds to the WhatsApp message to accept the role. During the “training week,” John had to click on a button to “submit orders” and earned 0.6% of the price of the app for each one. According to Digital Logic’s platform, this made €38 in less than 15 minutes.

After a week of training, John had to contact a customer service agent on Telegram to get a “random bonus” of €29. His account now had €66. John was then advised he had to set up a cryptocurrency wallet to get the funds. At this point he was asked to add €30 to get the second set of tasks. He was advised the account had to be funded to create a “real money flow data”. At this point John became suspicious and did not add any further money or complete the tasks.

John reports the matter to the actual recruitment agency who inform him that unfortunately he has been the victim of a scam operation.

Employment scams: **What can I do to prevent it?**

- Consider having a statement on your website that confirms that you are aware of the scam operating and that is not how your organisation would operate/communicate with potential applicants.
- Look out for negative reviews and feedback on social media sites to ensure that those that have posted are aware that it is a scam.
- Encourage those who think they have been scammed to stop all communication with the scammer immediately and report to JobsAware and Action Fraud.
- Ensure the use of job boards involved in third party schemes to demonstrate Online Safety Act compliance, such as the Online Recruitment Scheme.
- Develop best practice guidance to post on your marketing channels (e.g. your website, social media etc) that gives some tips on how to spot a scam message including:
    - It's a message that you weren't expecting.
    - It comes from a number or email address you don't recognise.
    - It contains a link to a website.
    - It offers unrealistic salaries or working arrangements - if it's too good to be true then it probably is.
    - It is asking for money or personal details.
    - The advert is poorly written and contains spelling errors.

Manipulation of artificial intelligence

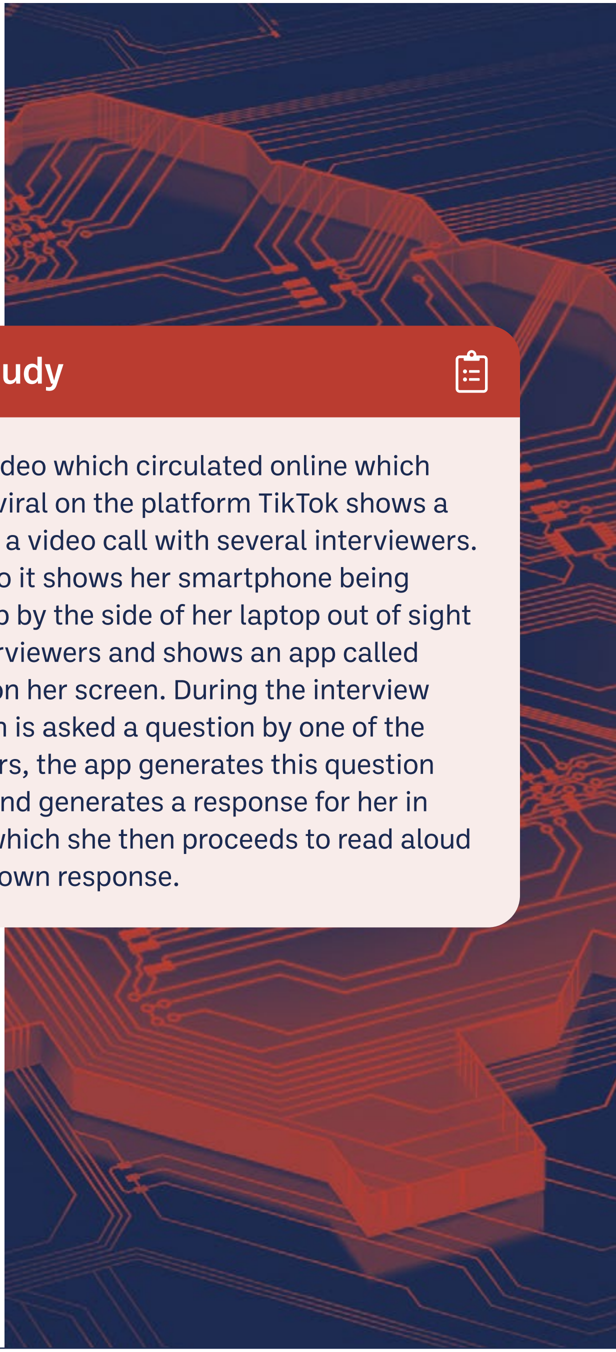
Includes deep fakes and virtual interviewing

Artificial intelligence (AI) is where technology can mimic human thinking and decision-making processes.

Although the use of AI generated interviews is an advantage for applicants, it can bring several disadvantages for employers. AI platform ChatGPT has been used by individuals to craft their CV's and to complete job application forms in a way which will give them a higher chance of securing a role. There have now also been many cases of applicants using AI generated platforms to help them with interview responses when these are conducted on a remote basis.

The issues that AI generated interview responses can cause for employers are:

- An applicant hired due to using AI but lacks the appropriate knowledge or skills and once they do start a job they can cause organisations a high risk, depending on the sector. For instance if the individual is working with vulnerable adults or children in regulated settings such as a hospital, or if they are working in a physical role and have no experience dealing with dangerous machinery and equipment and can therefore cause risk to themselves and others around them.
- The use of AI by applicants can lead to an unfair disadvantage for those who don't use AI but actually do have the appropriate skills and experience for a role but are not hired due to not responding in an expected way by hirers.



Case study

A recent video which circulated online which first went viral on the platform TikTok shows a woman on a video call with several interviewers. In the video it shows her smartphone being propped up by the side of her laptop out of sight of the interviewers and shows an app called 'AI Apply' on her screen. During the interview the woman is asked a question by one of the interviewers, the app generates this question instantly and generates a response for her in real time which she then proceeds to read aloud as if it her own response.

Manipulation of artificial intelligence: **What can I do to prevent it?**

You can mitigate the use of AI generated responses by:

- Utilise AI detection systems – the creators of ChatGPT have developed a tool called 'AI text classifier' designed to detect text generated by their chatbot, this tool can distinguish between human-generated and computer-generated text which identifies if an applicant has used AI assistance to craft their responses, or application materials.
- Consider competency-based interviews as opposed to structured interviewing (where answers can easily be generated). Competency-based interviews focus on probing the applicant about specific situations and will require them to delve deeper when providing responses which can be difficult to rely upon AI.
- Use methods which cannot be manipulated – consider conducting your interviews face to face as opposed to remotely, as this would make it impossible for applicants to cheat.
- Ensure you don't deploy AI in a way that mistreats work seekers. The Better Hiring Institute have created the UK's first Best Practice in the Use of AI in Hiring which can be found here.

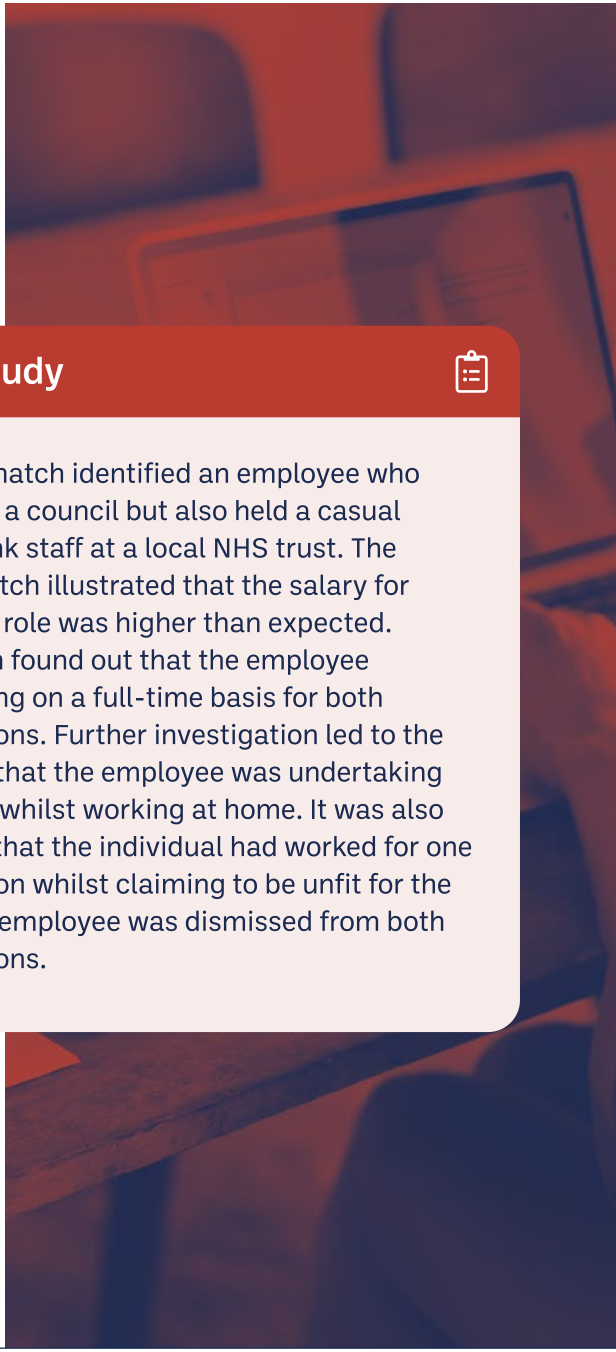
Dual employment

The Covid-19 pandemic has drastically changed the way we now work. Jobs that were once fully face to face have either now become fully remote or hybrid and has led to the rise of 'dual employment'.

Dual employment is the practice of working two jobs simultaneously and usually breaches workplace rules and contracts of both the primary and secondary employer. This differs to moonlighting, as this is where an individual is performing a side job in addition to another job which is typically done on a part-time basis.

The main issues that arise for employers due to dual employment is:

- Conflict of interest for your business – a competitor business could be gaining an advantage because of the employee working two jobs. This is more common for recruitment agencies that provide services for the same industry and within the same locations. For example, a remote admin assistant could be performing much better for one business than they are the other.
- Employee availability.
- Lower productivity and performance.
- Juggling tasks/duties/projects in both jobs is not an easy task and can thus lead to errors or disorganisation.
- Risk of confidential and sensitive data being leaked to a competitor which could damage your business.



Case study

A payroll match identified an employee who had joined a council but also held a casual role as bank staff at a local NHS trust. The payroll match illustrated that the salary for the casual role was higher than expected. It was then found out that the employee was working on a full-time basis for both organisations. Further investigation led to the discovery that the employee was undertaking both roles whilst working at home. It was also identified that the individual had worked for one organisation whilst claiming to be unfit for the other. The employee was dismissed from both organisations.

Dual employment: **What can I do to prevent it?**

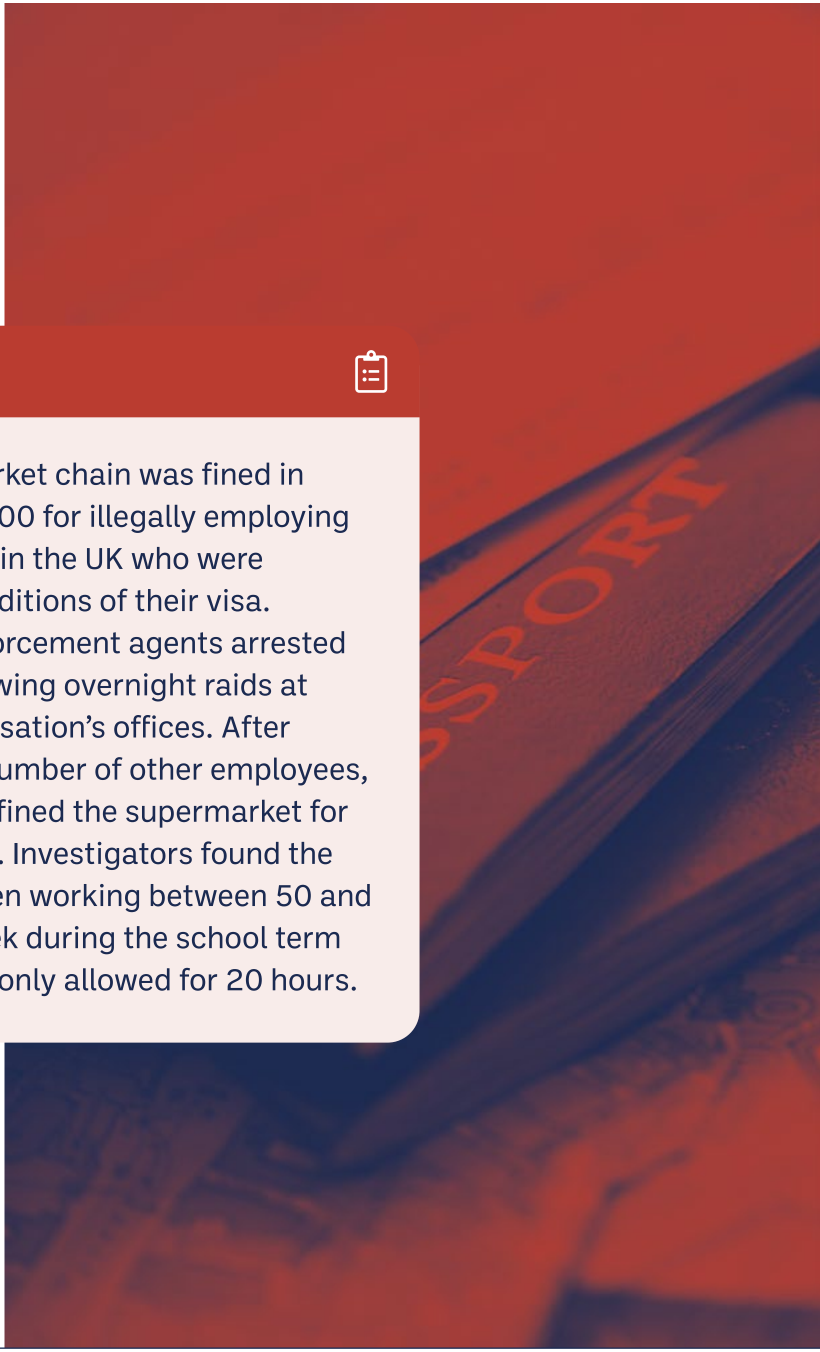
Although it is not completely possible to prevent employees taking on a second job, there are steps to take which can mitigate the chances:

- Revising employee agreements/contracts which use language that restricts 'dual employment' and illustrates your organisations expectations. Doing so communicates to new starters and current employees that time theft and dishonesty are not prohibited within your organisation.
- Seek references for all new starters which may highlight any secondary employment concerns.
- Consider conducting overemployment monitoring checks at point of employment to confirm other employment positions held. Many employee screening companies in the UK can perform these checks on your behalf.
- Screening checks for current employees in specific roles could be done regularly, as a minimum every 12 months by an outsourced screening company, or utilising internal hiring teams.
- Monitor your employees' performances to track delays in tasks, as well as repeated errors.
- When screening a potential new starter, you could utilise application forms to carefully screen the individual's current position and question them about their status pre and post employment.
- HMRC documents and open banking statements could be used to find out information on secondary employment.

Immigration fraud

Immigration fraud occurs when dishonest means are used to obtain illegal entry into the UK or to remain in the country past the legal limit. This can include using a false or altered document to support a visa application, with the intention of breaching UK immigration law.

Examples of immigration fraud includes entering without leave, overstaying, failing to observe conditions of leave, forgery of documents and working outside of the visa restrictions.



Case study

A large supermarket chain was fined in excess of £115,000 for illegally employing foreign students in the UK who were breaking the conditions of their visa. Immigration enforcement agents arrested 20 workers following overnight raids at one of the organisation's offices. After investigating a number of other employees, the Home Office fined the supermarket for 23 of its workers. Investigators found the students had been working between 50 and 70 hours per week during the school term when their visas only allowed for 20 hours.

Immigration fraud: **What can I do to prevent it?**

There are several ways to prevent employing illegal immigrants through conducting adequate right to work checks and ensuring you have robust monitoring processes in place.

Digital checks

- For workers with a valid British or Irish passport, a digital right to work check can be carried out using 'Identity Document Validation Technology' (IDVT) via an 'Identity Service Provider' (IDSP) which produces a digital identity verification element of the check.
- Digital RTW checks are the safest and fastest way of preventing illegal working, with average times for some IDSP products being under 3.5 minutes to complete the check.
- If looking to outsource these checks, you should pick a reputable provider that stay up to date with the latest changes at government level.
- A full list of certified IDSP providers can be found here.

Reed Screening

Data from Reed Screening from a recent study of over 130,000 identity and right to work checks conducted shows:

- 90% of these showed a pass rate
- The average time taken to complete the check was 3 minutes, 14 seconds
- 94% are completed within 48 hours of the initial link being sent.

Click here to find out more.

Online/share code checks

- For use with those with a valid visa. A share code will be provided and an online check can be conducted along with a video call to verify that the person you are doing the check matches the photo on the visa.

Manual/in-person checks

- Dependent on the type of document, you should obtain a copy of the original, check the validity for obvious signs of forgery and retain a clear copy, either electronically or in hardcopy and record a date in which the check was conducted.

Best practice tips

- Click here for full Home Office guidance on other checks that can be carried out.
- You can also contact the Home Office:
  Employer Enquiry helpline
  Telephone: 0300 790 6268
  Monday to Thursday, 9am to 4:45pm
  Friday, 9am to 4:30pm

When you have obtained an individual's document you should ensure:

- The document is genuine, original and hasn't been tampered with.
- The photographs of the individual, names and dates of birth are consistent across multiple documents.
- All records of right to work checks must be recorded for at least two years after the employee leaves their employment.

Be aware

- Hiring staff should be trained on how to conduct adequate right to work checks. For example since the move to digital, there has been an increase in the use of fake birth certificates in order to obtain work. Things to look out for when spotting a fake birth certificate are:
  - Poor quality/blurry text.
  - Incorrect spelling or grammar.
  - Unusual format – the issuing authority will have a standard format that can be checked online.
  - Only the surname should be entered in upper case, not the forename(s).
  - Dates of birth should be shown with the day and month in words and the year in figures.
  - No raised seal – real birth certificates will either have a raised seal or stamp.
  - If you have any concerns with the document, you should contact the issuing authority to verify the document's authenticity.

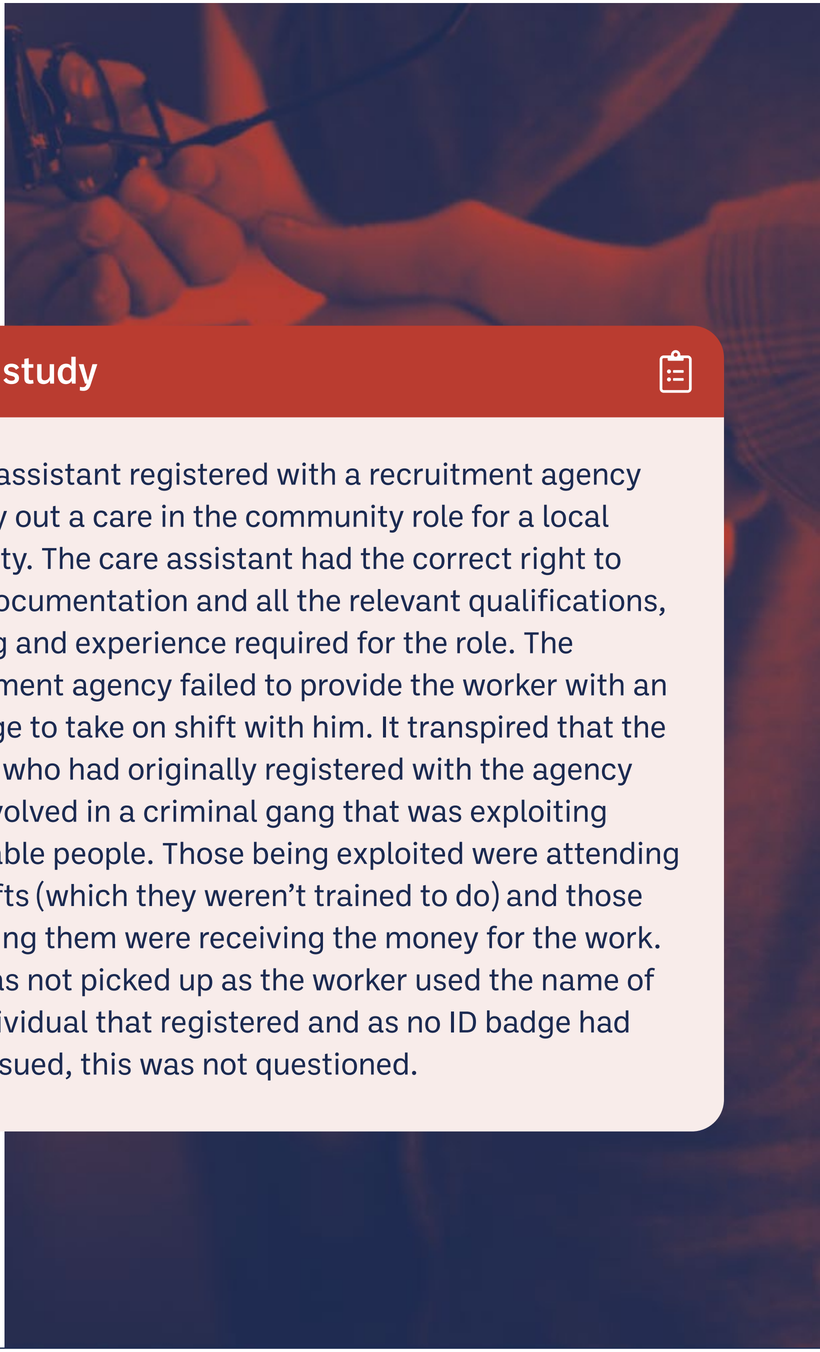
Fraud as a result of recruitment agency usage

Part 1: Worker impersonation

Worker impersonation normally occurs via a recruitment agency. It is where the individual who has registered with the agency and is suitably vetted for a role will send another person on their behalf to complete their assignment/shifts. This could be facilitated for the purpose of modern slavery as the person getting paid for the work isn't actually doing it but using others (and likely paying them a small amount) to complete the actual work.

This can pose many different risks to your organisation, such as:

- Higher likelihood of accidents occurring if the individual isn't qualified or skilled for a particular role.
- Posing a safeguarding risk to vulnerable adults or children.
- Reputational damage.



Case study

A care assistant registered with a recruitment agency to carry out a care in the community role for a local authority. The care assistant had the correct right to work documentation and all the relevant qualifications, training and experience required for the role. The recruitment agency failed to provide the worker with an ID badge to take on shift with him. It transpired that the worker who had originally registered with the agency was involved in a criminal gang that was exploiting vulnerable people. Those being exploited were attending the shifts (which they weren't trained to do) and those exploiting them were receiving the money for the work. This was not picked up as the worker used the name of the individual that registered and as no ID badge had been issued, this was not questioned.

Worker impersonation: What can I do to prevent it?

This can be a challenging situation to overcome as the recruitment agency has registered the individuals, therefore you may not have carried out an interview of the candidate yourself. However, the below will help to mitigate the risk.

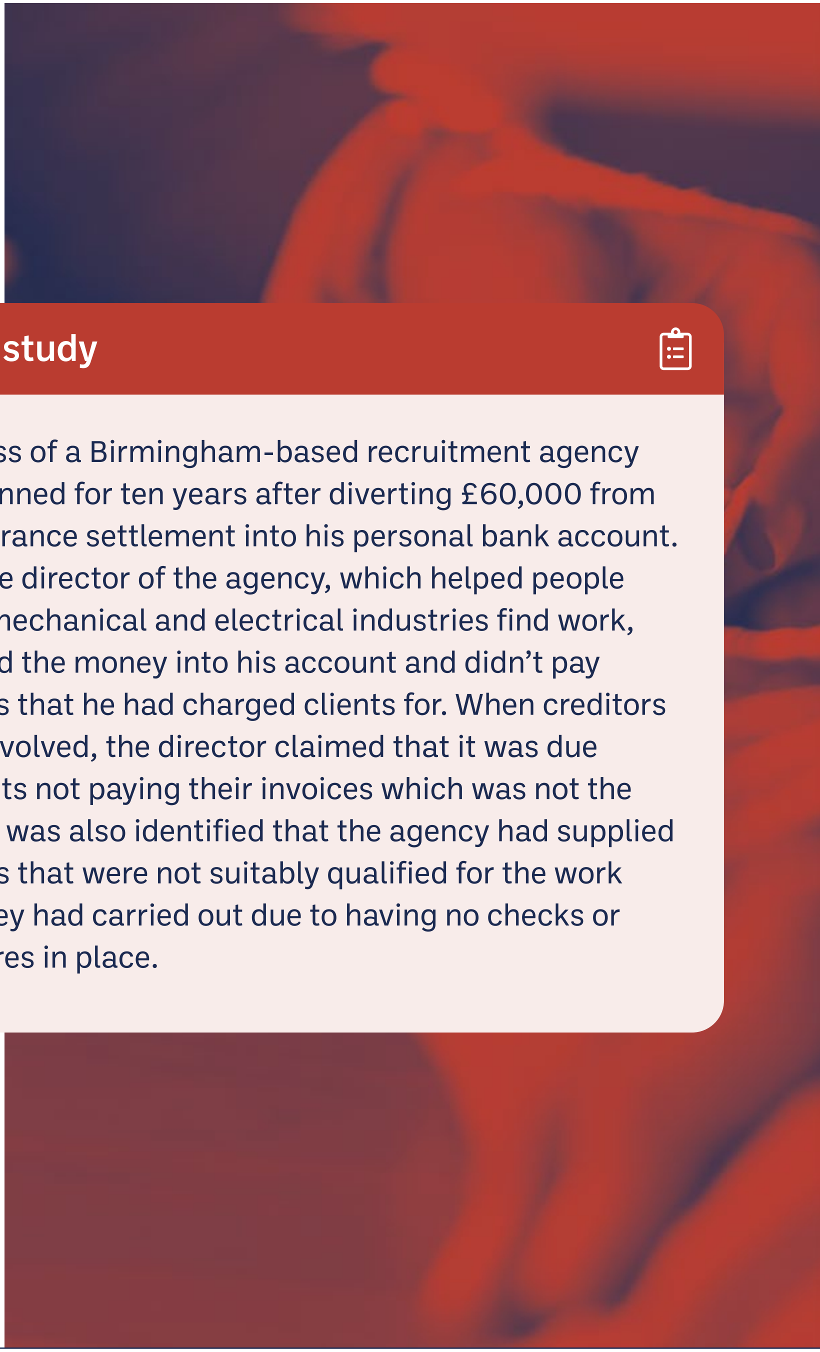
- Use a reputable recruitment agency that are registered with either the REC or APSCo (who are accredited trade bodies for their industry). This will ensure they uphold certain compliance standards and are regularly audited.
- Require candidates to provide identification documents on arrival of their first shift so you can verify this with what the agency has provided to you.
- Insist that an ID badge is issued by the agency, particularly in regulated settings where there may be a safeguarding risk.

Part 2: Use of non-compliant agencies

Recruitment agencies play a very important part in staffing requirements for organisations across multiple industries. Whilst the sector is governed by legislation and regulated by the Employment Agencies Standards Inspectorate, there are still a concerning number of agencies that are set up and operate without following the rules.

As the intermediary between you and the staff that are supplied to you, it is important that you are assured that the correct measures are in place to prevent potential fraudulent activity by individuals before they start with your organisation.

A recruitment agency should be carrying out robust vetting checks on the workers that they engage before they are referred to you. This should identify any anomalies in identity and right to work checks, employment history and referencing, qualifications and any additional requirements as agreed with your organisation and the agency. Knowing that the agency you engage with is compliant will reassure you that your workforce has been thoroughly checked.



Case study

The boss of a Birmingham-based recruitment agency was banned for ten years after diverting £60,000 from an insurance settlement into his personal bank account. The sole director of the agency, which helped people in the mechanical and electrical industries find work, diverted the money into his account and didn't pay workers that he had charged clients for. When creditors were involved, the director claimed that it was due to clients not paying their invoices which was not the case. It was also identified that the agency had supplied workers that were not suitably qualified for the work that they had carried out due to having no checks or measures in place.

Use of non-compliant agencies: **What can I do to prevent it?**

- Use a reputable recruitment agency that are registered with either the REC or APSCo (who are accredited trade bodies for their industry). This will ensure they uphold certain compliance standards and are regularly audited.
- Question the compliance checks that the recruitment agency have in place as part of your onboarding due diligence process.

About Us

The Better Hiring Institute is a not-for-profit social enterprise driving the development of a modern, agile UK labour market, accelerating economic recovery. Working closely with all the major UK industries, The Better Hiring Institute is driving standardisation, best practice, and digital innovation to reduce hiring times, enable portability, and improve safeguarding. Cross industry themes include digital standardised referencing, open banking, digital right to work checks, education credentialing, and digital identity. The Better Hiring Institute is already working with many of the UK's largest, household names making UK hiring the fastest globally.

Reed Screening are the leading specialists in pre-employment vetting and are at the forefront of influencing regulation and industry change. Reed Screening are the only UK, onshore screening company who are open 24/7, they are family owned and give 20% to charity. Their business never sleeps so if you ever need them, they're available. Their vision is to 'create a safer world at work' by collaborating with government bodies and industry leaders to bring about change.

Cifas is the UK's fraud prevention service, leading the fight against fraud by sharing data, intelligence and learning. With over 30 years of experience in fraud prevention and financial crime, Cifas works with a range of UK businesses, charities, and the public bodies to help them protect themselves, their customers and the public, delivering trusted data of unparalleled depth and diversity, and hosting the largest databases of fraud risk in the UK.

Dr Suzanne Smith (PhD), founding director of ST Smith Safeguarding Consultants Ltd, has over 32 years in safeguarding. Her company concentrates on providing advice, support, training, policy development and independent reviews for all concerns relating to safeguarding adults and children. With an unrelenting focus on quality and excellence in safeguarding practice across a variety of public, private and public sector organisations, ST Smith Safeguarding Consultants Ltd are steadfastly outcomes focused, placing children and adults at risk at the centre of all they do. As a member of the Better Hiring Institute Advisory Board, Suzanne is always thrilled to be part of BHI events and publications and be part of their vital work to improve safeguarding.

We would like to thank all of the contributors to this guidance. As we continue to tackle the ever changing threats of Hiring Fraud, please report any new trends in this space to secretariat@ betterhiringinstitue.co.uk as we look to keep this guidance as reflective as possible of the current UK hiring landscape.

Click here to access the Better Hiring Institutes other industry leading guidance.