Tackling Hiring Fraud

The Essential Guide for UK Business on Making Hiring Safe

In collaboration with:

Reed Screening

NCA National Crime Agency

STOP! THINK FRAUD

BHI

beruku

cifas Fighting Financial Crime Together

Fullbrook Strategies

Foreword

Rt Hon Lord Hanson of Flint
Minister of State

Statistics show that fraud continues to increase in the UK and a robust, joined-up approach is needed if we are to turn the tide.

Hiring Fraud is no different, whether it's employment scams targeting undergraduates, the misuse of AI to fool organisations into hiring bad actors, or immigration fraud undermining business and Government's efforts to reduce illegal working. To tackle this, business, government, and law enforcement need to work together in a unified way.

This is why I am delighted to support the work of the Better Hiring Institute in developing this guide for UK employers on how to protect themselves, the public, and national infrastructure from the threat of Hiring Fraud. Accelerating data-sharing and collaborative working will help industry stop, block, and disrupt fraud and harm. Working together will be a key aspect of the new and expanded Fraud Strategy designed to deepen partnerships to reduce fraud.

Hiring Fraud is an entry route for scammers and criminal gangs to cause significant harm. This could take the shape of Fake IT workers planted in businesses to cause cyber attacks, it could be fake recruiters using the jobs market as a way to reach the public, or ways for bad actors and groups to infiltrate organisations to cause widescale financial fraud. By improving the defences of UK firms, we can help prevent significant harm. By working together and using emerging tech such as AI to fight crime, we can encourage job boards to remove fake job adverts from their platforms.

I sincerely hope businesses take heed of this free guide and use it to help protect themselves, the public, and become part of a joined up national approach to tackling fraud in all its guises.

Introductions

Simon Fell

Director, Fraud and Financial Crime Fullbrook Strategies

Former UK Government Anti-Fraud Champion

No sector is immune to the threat of fraud. On a regular drumbeat we hear of more and more high-street names being exploited by organised crime groups – taking down key infrastructure for profit and sport. It may be inconvenient not to be able to access your online banking, or to place an order from your favourite brand while firewalls are re-built and systems patched, but there is something more insidious going on – the exploitation of our data for onward criminal gain.

These attacks aren't just hackers operating from overseas – they are often enabled by insiders giving information about internal systems and their weaknesses.

So, recruiters and employers need to be alive to these risks: of the huge cost to them of assets stolen; of the reputational damage they may face, and of the cost of rebuilding and in lost business.And there is another side of the coin too – for employees. Fake job adverts are becoming more and more prevalent. The now well-understood practice of money-muling has not gone away.

But new employment fraud trends are being established too. The National Protective Security Authority, a branch of MI5, recently warned about suspicious job adverts being placed by hostile foreign agents. And the Director General of MI5 said that professionals should be weary of a "tempting online job advert in your sector [that] is just too good to be true".

Too many businesses do not take these risks into account until it is too late. The cost of not doing so might not be measured simply in pounds and pence, but in the viability of their businesses as a going concern. That is why this guide matters and should be on every recruiter's desk.

Fraudsters are innovative and hungry. From money muling to insider fraud, old practices are being supercharged with the incredible technology of our age, enabling deep fakes of legitimate documentation, and fraud at volumes unimaginable just years ago.

This guide provides a comprehensive resource on how to protect yourself, your business, and your customers. Fraud affects us all, and we all have a part to play in preventing it. With the tools this guide gives you, you will be well-equipped to do so.

Keith Rosser

Director of Reed Screening

Chair of the Better Hiring Institute

The mission of the Better Hiring Institute is to make UK hiring faster, fairer, and safer. The rapid growth of hiring fraud has the potential to really undermine the ambition to make UK hiring the safest it can be. That's why I am so proud of this work, because it's critical to help UK employers turn the tide on hiring fraud.

In 2023 the Better Hiring Institute, Reed Screening, and Cifas published the world's first guide on hiring fraud and now, 2 years on, to commemorate International Fraud Week the Hiring Fraud 2.0 guide has launched in Parliament with Fraud Minister, Lord Hanson, Rishi Sunak's former Anti-Fraud Champion, Simon Fell, and over 200 Parliamentarians, employers, and experts.

Whilst updating on key threats such as the use of Reference Houses for fake references, more traditional forms of hiring fraud such as CV and Qualification fraud, this guide brings on the most up to date threats we – as employers – face, such as Fake IT Workers many of whom are sponsored by the North Korean state, Dual Employment, and the misuse of AI.

I am delighted by the role Reed Screening continue to play as leaders in this field, and through the partnership with Beruku, Cifas, and the Better Hiring Institute I'm proud to support this all-important guide to help employers across the country protect themselves from harm.

Introductions

Mike Haley
CEO of Cifas

Fraud is now the most experienced crime in the UK, accounting for 44% of all offences. It costs the UK economy an estimated £219 billion a year. In 2024 alone, Cifas members prevented over £2.1 billion in fraud losses – and the threat is growing.

Hiring fraud is a key part of this evolving landscape. In the first half of 2025, overall cases recorded to the Cifas Threat Database surged by 32% compared to the previous year, with organisations reporting a rise in employees working multiple jobs without consent (polygamous working), using fraudulent reference houses, and even being placed by organised crime groups as insiders or 'innys'.

Our Workplace Fraud Trends survey – which launched in October 2025 – revealed that one in five employees admitted to polygamous working, 30% felt it was acceptable to use fake references, and 24% had committed expenses fraud.

These insights suggest a shift in workplace norms and raise urgent questions about organisational culture, risk management, and accountability.

Hiring fraud is not just a compliance issue – it's a business risk. Fraudulent hires can lead to data breaches, financial loss, reputational damage, and regulatory penalties. And with regulatory shifts – including the new offence of Failure to Prevent Fraud - placing more liability on businesses, the cost of fraud is increasingly being borne by employers.

Organisations must act now to build strong counter-fraud cultures – prioritising prevention, educating employees, and embedding fraud resilience into hiring practices. By sharing intelligence across sectors, businesses can spot fraudulent candidates before they gain access to sensitive systems or data.

With the right tools, training, and reporting mechanisms in place, employers can detect and deter insider threats – protecting their operations and their people.

However, it's important to stress that no business is immune to fraud, and no organisation can tackle it alone. Collaboration is critical. That's why we're proud to partner with the Better Hiring Institute on this essential toolkit – helping UK employers build safer, smarter, and more fraud-resilient hiring strategies.

> **An uncertain employment market represents a perfect storm for employment scammers as they heartlessly exploit honest people – who simply want to find work to pay for life's essentials or put aside a little more for well-earned extras. And when people start looking for opportunities which they may not normally consider, they inadvertently become perfect fraud targets.**
>
> **By collaborating with Lloyds Banking Group and JobsAware, our new Job Seekers Tool Page will help individuals see the difference between a fake and genuine work opportunity and ensure when they apply, they're not falling for a scam.**
>
> Tony Neate, CEO of Get Safe Online

About this guide

This is a 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 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:

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 are experts in tackling Hiring Fraud with systemised fraud detection checks built in.	✓ 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 fraud.	
Address the issues of those being scammed by fake jobs by linking to the Get Safe Online, Lloyds Banking Group, and JobsAware free jobseeker portal on Careers Pages.	
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 and Reference Houses

A "Reference House" is a term that defines a fraudulent organisation providing fake references to an individual for a price.

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 fictitious 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.

Reed Screening owns and operates an ever-growing database of over 2,000 known Reference Houses which has grown by 25% in the last 3 months alone.

Cifas' Workplace Fraud Trends 2025 report shows that almost a fifth (19%) say they or someone they know has used fraudulent Reference Houses to cover employment gaps, in the last 12 months.

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?
- Call the organisation to check its genuineness.

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). Reference Houses are often on Companies House so check that the content looks genuine, for example number of employees.
- 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 tell-tale 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.

In a survey commissioned by Hedd and carried out by YouGov in April 2025, 58% of respondents verify their applicants’ degree credentials.

The larger the firm, the more likely it is that they will verify degrees – 85% of large companies and 76% of medium-sized companies do it compared to just 39% of small firms.

45% of large recruiters had found a candidate giving false information about their qualifications.

68% of large firms said that AI had increased application fraud.

Unsuccessful false employment applications accounted for 33% of all member filings to the Cifas Insider Threat Database between January to June 2025 – making it the second most dominant case type.

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 tell-tale 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.
- Contact 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: Hedd | Appruvr
- Train your hiring team on how to check the authenticity of certifications, for instance being able to spot common red flags.
- When using recruitment agencies ensure they have robust vetting and checking systems. Align contingent worker vetting to permanent vetting and screening processes to prevent bad actors infiltrating your organisation through other routes.

More solutions to help tackle qualification fraud here:

Vision supports organisations in managing employee risk and monitors behavioural changes in real time.

Insider Threat Protect helps target internal risks through data, intelligence, and learning.

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.

AI-generated fake documents including fake IDs and personal information are on the rise. AI-driven tools, such as ChatGPT and CoPilot, and image generators are increasingly being used, with minimal input, to generate very convincing replicas of official identity documents. Passports, driver's licences, and birth certificates are now easily counterfeited using digital tools that are widely available.

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.

Over 21,700 false applications were recorded to the Cifas National Fraud Database in 2024, an increase of 10% on 2023. You can read more in Cifas' Fraudscape 2025 report.

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

When checking documentation as part of the application process, there are tell-tale 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.
- Artifacts of digital editing such as duplication of pixelation, distortion of the image specifically colours, font and text size inconsistencies, irregularity of formatting, and a lack of metadata in the digital file.

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 identity documents and certifications, for instance being able to spot common red flags for flase documents.
- Consider membership in or use of fraud prevention services that specifically focus on forged or stolen documents such as Amberhill, Cifas, SIRA, and specialist identity document and fraud training in alignment with UK Government best practice, for example with organisations like Beruku Knowledge.

CV based fraud

Includes falsified employment history and 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 of time spent in prison.
- Exaggerating salary levels.

New Hedd research has shown how employers are becoming increasingly concerned with job applicants using AI tools to embellish or falsify their credentials. As thousands of new graduates enter the labour market, a YouGov survey for Hedd reveals a sharp rise in CV fraud, with employers warning that AI is making it easier for candidates to falsify job applications.

Degree verification and fraud service provider Hedd, part of Jisc, commissioned YouGov to poll more than 500 HR decision makers. It found that 67% of large companies have seen an increase in job application fraud, attributing the trend to AI tools being used to enhance or fabricate experience or qualifications.

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 for 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 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 and social media/ SMS messaging scams

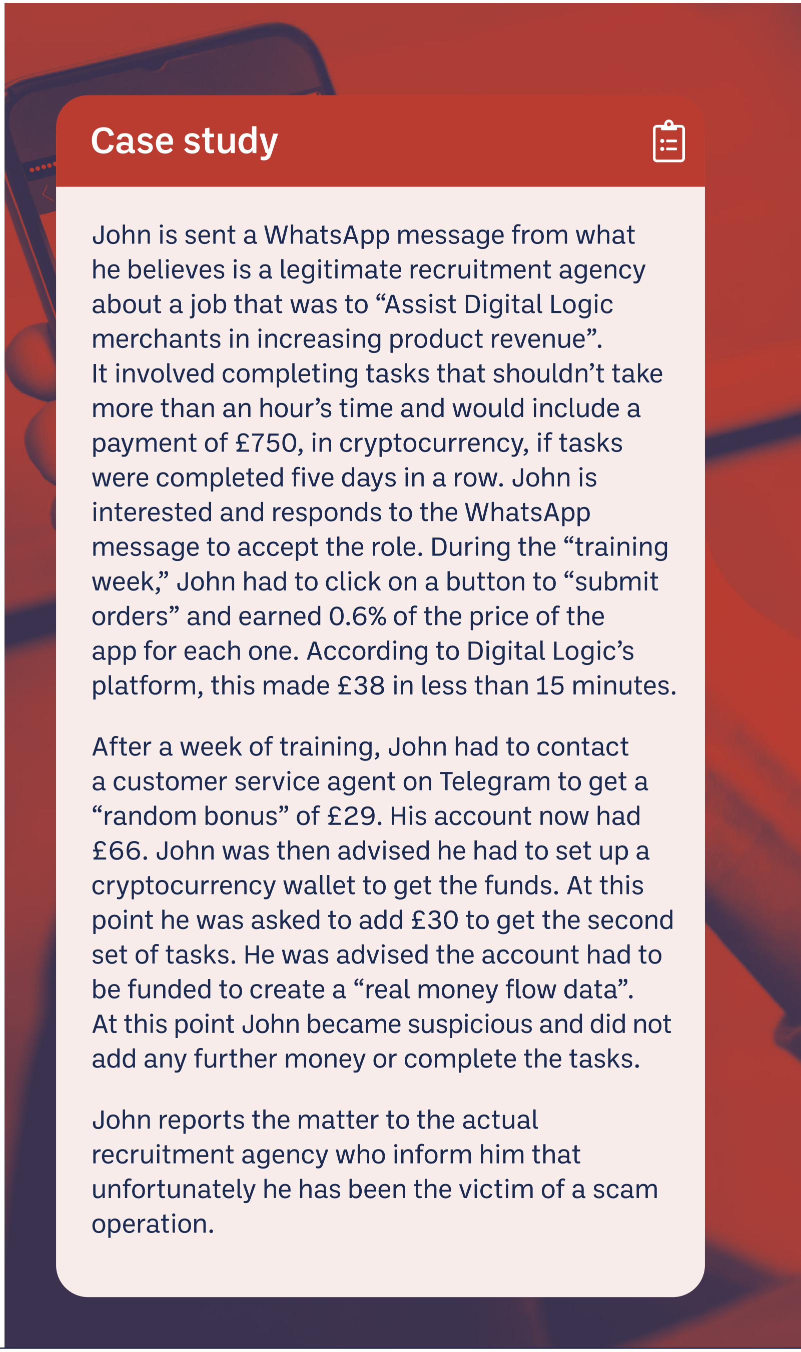
Employment or recruitment scams have risen significantly in recent years. Action Fraud data showed a doubling of reports of recruitment scams in two years (2094 in 2022 vs 4876 in 2024) and Lloyds Banking Group have indicated a 237% rise in cases reported to them in 2025.

Employment scams facilitate a variety of different types of fraud including identity theft, financial scams, and 'money muling'. Fraudsters use legitimate-looking job adverts, often pretending to be on behalf of well-known brands, advertised on job boards or social media platforms. Then direct contact with the jobseeker by email, text, messaging apps such as WhatsApp, or LinkedIn messenger is a popular method to entice them into believing the job is real.

Commonly fraudsters will steal personal details from jobseekers via CVs or the application process, or will dupe job seekers into paying for employment-related services such as criminal record checks, training, travel, or uniform and equipment.

In some cases, fraudsters trick jobseekers into believing they have been appointed into a real role and the person works without being paid for a period, or is duped into facilitating further fraud. In most serious cases, employment scams are a gateway into modern slavery.

In 2025, the Online Safety Act ("OSA") came into force which requires platforms such as job boards to comply with the legislation and protect people from fraudulent adverts. JobsAware have developed the world's first Online Recruitment Scheme, a certification that job boards can use to demonstrate their compliance to the OSA. Some platforms have already signed up and taken steps to protect job-seekers. Additionally, platforms such as LinkedIn have issued public guidance about staying safe on their platform.



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 those that have posted are aware 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

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

Virtual interviewing

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 CVs 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.

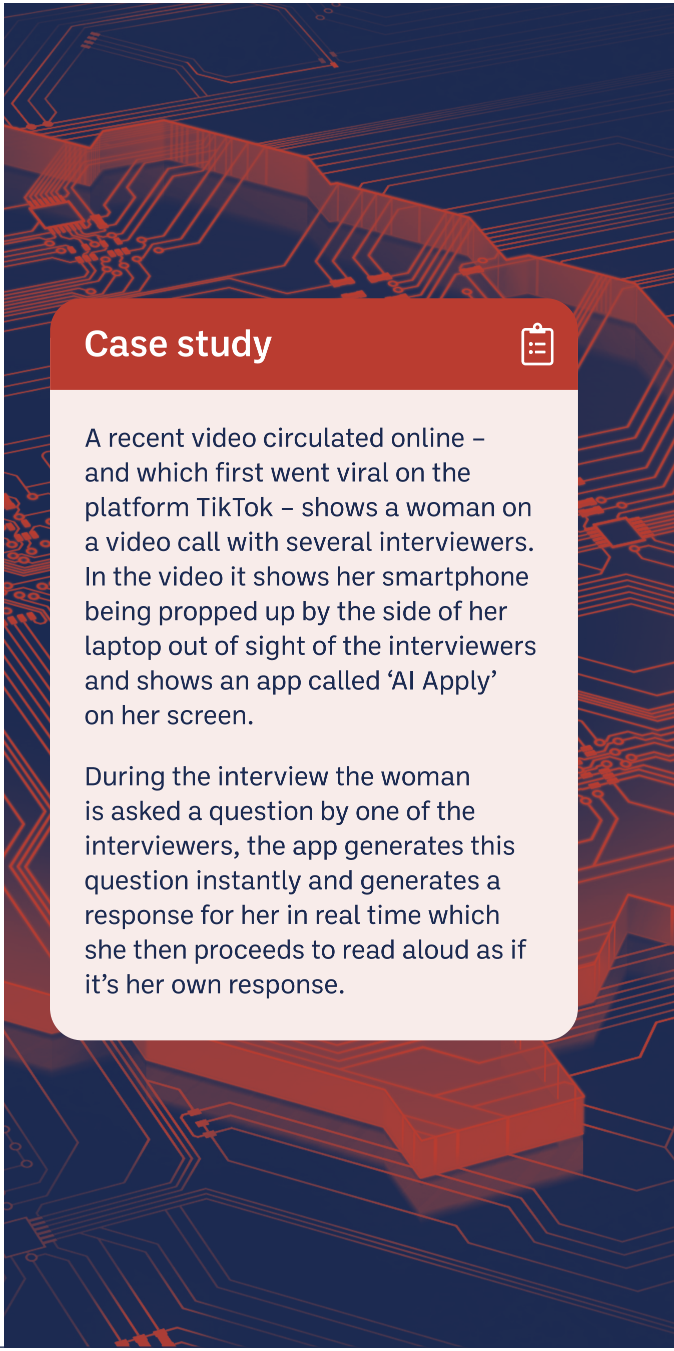
The issues that AI generated interview responses can cause for employers are:

- An applicant could lack the appropriate knowledge or skills, potentially with significant consequences, dependent on the sector. For instance if they are working in a regulated setting e.g. a school/hospital or in a specialist manual role operating dangerous machinery, therefore causing risk to themselves and others around them.
- The use of AI by applicants can lead to an unfair disadvantage and unintended bias for those who don't use AI but do have the appropriate skills and experience for a role but are not hired due to not responding in an expected way by hirers.

Deepfakes/Avatars

Around 17% of hiring managers globally reported encountering suspected deepfake interviews by the end of 2024, a notable jump from just 3% the previous year.

85% of identity fraud attempts in 2024 involved AI generated or manipulated content, indicating deepfakes are a primary tool in broader fraud efforts. One survey in the UK found that 29% of job seekers had used AI to generate interview answers, and 27% used it to complete test assignments, showing widespread AI use in the application process, which can facilitate more sophisticated deepfakes.



Case study

A recent video circulated online – and 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's 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 via AI.
- Use methods which cannot be manipulated – consider conducting your interviews face to face as opposed to remotely, as this would make it difficult 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.

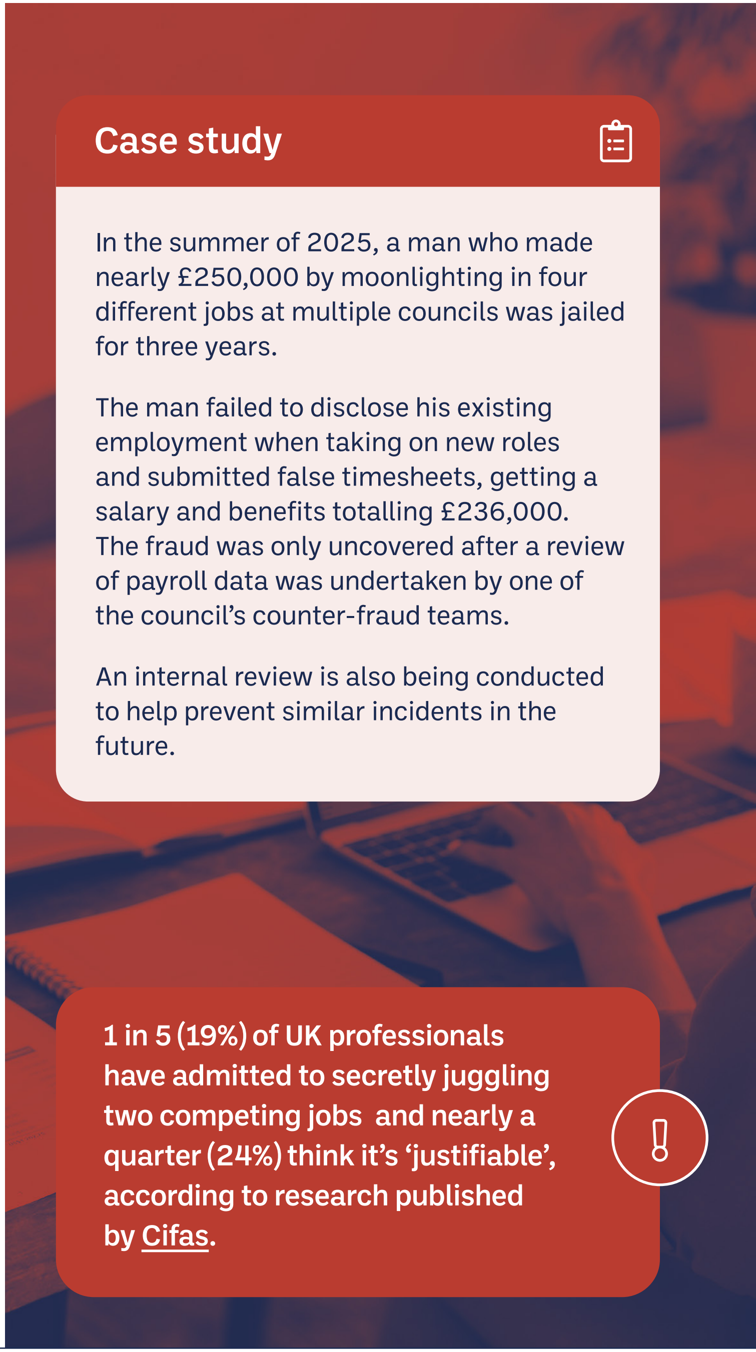
Dual employment

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.

A 2025 report by the UK's leading fraud prevention service Cifas, found that 19% of employees have admitted to working two jobs secretly, with 24% believing this practice is justifiable. Social media platforms like TikTok and Reddit have also contributed to the trend by sharing tips on how to manage multiple roles.

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

In the summer of 2025, a man who made nearly £250,000 by moonlighting in four different jobs at multiple councils was jailed for three years.

The man failed to disclose his existing employment when taking on new roles and submitted false timesheets, getting a salary and benefits totalling £236,000. The fraud was only uncovered after a review of payroll data was undertaken by one of the council's counter-fraud teams.

An internal review is also being conducted to help prevent similar incidents in the future.

1 in 5 (19%) of UK professionals have admitted to secretly juggling two competing jobs and nearly a quarter (24%) think it's 'justifiable', according to research published by Cifas.

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 organisation’s 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.

Beruku Knowledge research has identified over 7,000+ false identity documents that have been advertised for sale through social media websites.

25% Passports

12% Residence Permits

12% National ID Cards

17% Visas

34% Driving Licences

Case study

Arrests for illegal working have soared to their highest levels since records began, following an uplift in enforcement action.

Under Operation Sterling, the government invested £5 million into Immigration Enforcement, to target, arrest, detain, deport and return illegal workers in takeaways, fast food drivers, beauty salons and car washes.

New figures show more than 8,000 illegal migrants have been arrested after 11,000 raids were carried out by Immigration Enforcement from October 2024 to September 2025.

Marking the largest enforcement crackdown on illegal working since records began, the data reveals a significant increase year on year of 63% and 51% for arrests and visits, respectively. Over 1,050 foreign nationals encountered on these operations have been removed from the country.

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.

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.

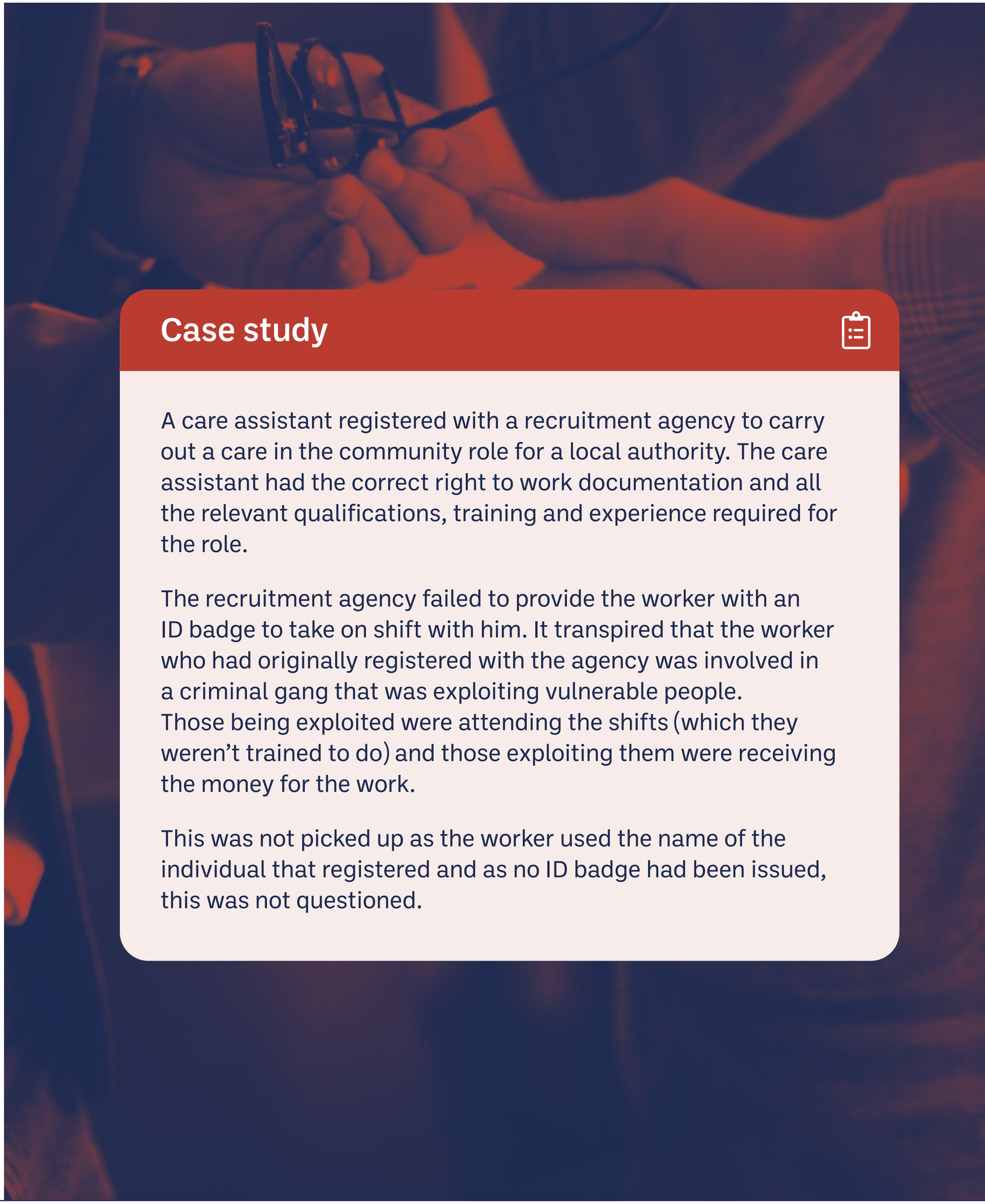
Fraud as a result of recruitment agency usage

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.

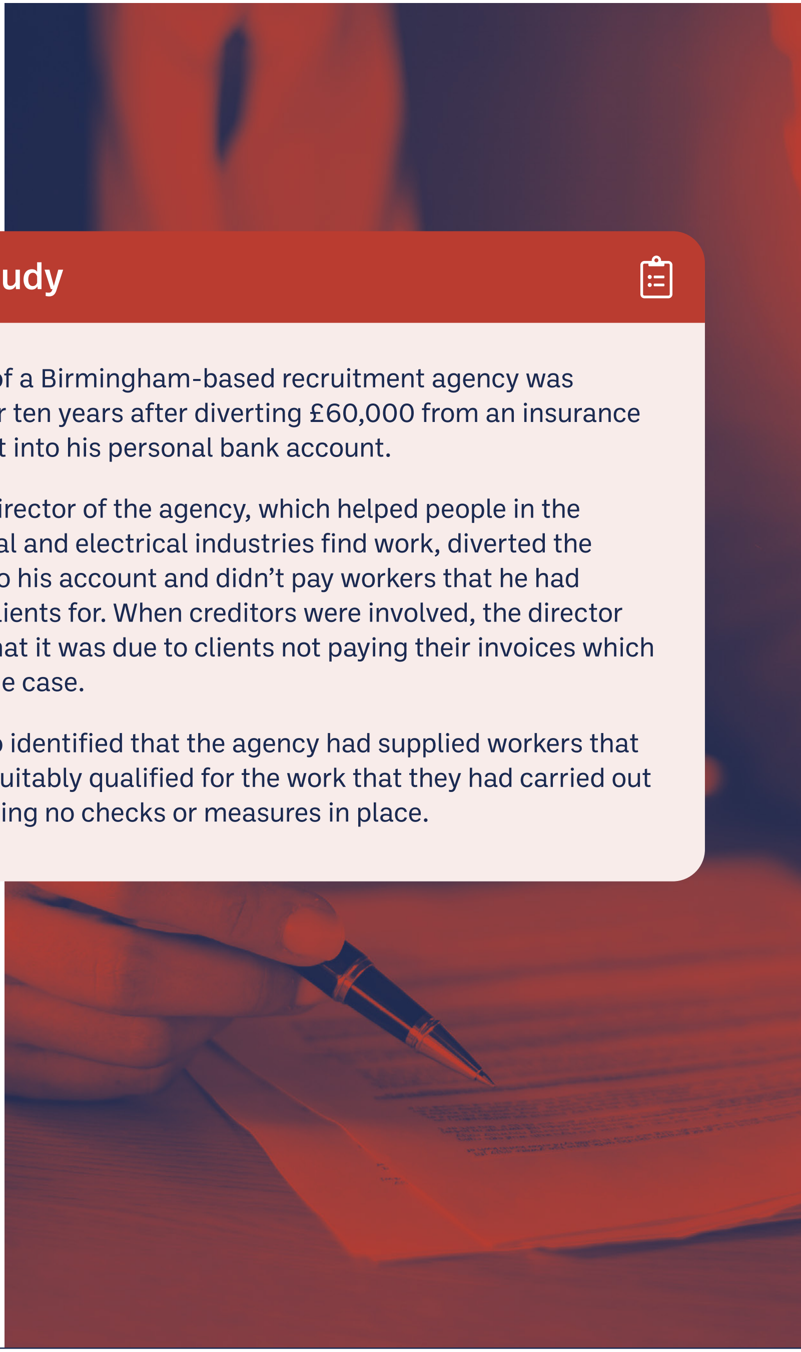
- Use a reputable recruitment agency that are registered with either the REC or APSCo (who are accredited trade bodies for their industry). This will ensure they uphold certain compliance standards and are regularly audited.
- Require candidates to provide identification documents on arrival of their 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.
- Ensure any recruitment agencies used can demonstrate effective vetting processes. Ask to see evidence that temporary workers are correctly checked and/or consider insisting recruitment companies use the same vetting processes as the end client.

Part 2: Use of non-compliant 'supply chain partners'

Recruitment supply chains play a very important part in staffing requirements for organisations across multiple industries. A recruitment supply chain usually contains a primary recruitment agency – in some cases it may include multiple recruitment agencies and also umbrella companies. It may not always be clear how many operators are in a supply chain. Whilst the sector is governed by legislation and regulated by the Employment Agencies Standards Inspectorate, there are still a concerning number of operators that are set up and operate without following the rules.

The primary recruitment agency is the intermediary between you, the end client, and the staff that are supplied to you. It is important that end clients are assured that the correct measures are in place to prevent fraudulent activity. If not, there is a risk that fraud could be conducted both by the individuals that are sent to work for you (if the agency doesn't background check them sufficiently) or even by the supply chain operator themselves, if they are non-compliant with recruitment legislation.

A recruitment agency under the Conduct Regulations 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 should 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 including their policies around engaging workers through umbrella companies.
- Report recruitment agency issues to the Employment Agencies Standards Inspectorate in Government until April 2026, from then report issues to the new Fair Work Agency.

Fake IT workers

Fake DPRK (Democratic People's Republic of Korea) IT workers have increasingly infiltrated UK company infrastructure by exploiting vulnerabilities in the hiring process, whether via recruitment agencies, direct employment, or as shadow staff within third party service providers. These workers, tend to apply for remote IT worker positions, across a variety of sectors, to make it easier to obfuscate their identity. This is not exclusive to just the IT sector, as most companies will now employ developers, software engineers, etc.

This tactic has been observed globally, and more recently has become prevalent in the UK. According to the Office of Financial Sanctions Implementation (OFSI) within HM Treasury it is almost certain that UK firms are currently being targeted by Democratic People's Republic of Korea (DPRK a.k.a. North Korea) IT workers disguised as freelance third-country IT workers to generate revenue for the DPRK regime. This in turn, can leave companies vulnerable to extortion, malware operations, sanction evasions, as well as reputational damage.

OFSI believes it is highly likely that DPRK IT workers are presently using online freelance platforms or job marketplaces to advertise their services to secure employment with UK firms.

DPRK IT workers are using aliases, false or fraudulent personae and proxies, to mask their true identities and hide links to the DPRK, often making them difficult to detect.

Fake DRPK IT workers may gain privileged access to sensitive or critical corporate information, which could lead to catastrophic results in terms of cyber security.

DPRK IT workers have been known to go undetected, which means the host company will have been employing the DPRK regime without realising. This is of course sanction evasion, but also puts the company at huge risk in terms of their system security, data privacy and leaves the company vulnerable to compromise.

There is a realistic possibility that this could result in information being compromised or misused.

Case study 1

In late 2024, one IT worker operated at least 12 personas across Europe and the United States. The worker actively sought employment with multiple organisations throughout Europe, particularly those within the defence industrial base and government sectors.

This individual demonstrated a pattern of providing fabricated references, building a rapport with job recruiters, and using additional personas they controlled to vouch for their credibility.

Fake IT workers:
What can I do to prevent it?

Recommendations related to the DPRK specifically:

The Office of Financial Sanctions Implementation recommend that UK firms hiring IT workers should:

- Use reputable online freelance platforms that offer robust verification measures of remote workers.
- Be vigilant against requests to communicate outside the original freelance platform website.
- Conduct video interviews and ensure workers are vetted by a reputable screening company, insisting for their audio and camera to be on.
- Require freelancers to shut off commercial VPNs when accessing company networks.
- Monitor the IP addresses of remote workers.
- Consider disabling remote collaboration applications on computers supplied to freelance remote workers.
- Flag remote workers who cannot receive equipment at the address listed on their ID documents.
- Use extra caution when interacting with freelance developers through remote collaboration applications.

For overall cyber security best practice:

- Review password policies and reset procedures for robustness, for example, require a call-back to a pre-registered employee phone number for all password/MFA resets.
- Ensure all hardware and software is up to date with the latest security protocols and bug fixes.
- Ensure backups are in place for all core systems and check with any cloud provider that you use to ensure you are covered by relevant back-up policy.
- Ensure best practice and workforce education in line with NCSC's 10 Steps to Cyber Security.

About Us

The Better Hiring Institute (BHI) 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 BHI 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 BHI is already working with many of the UK's largest household names to make UK hiring faster, fairer, and safer.

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 'pioneer the future of hiring' by collaborating with government bodies and industry leaders to bring about change.

Cifas is the UK's leading not-for-profit fraud prevention service with nearly 800 members from across key economic sectors including banking, retail, insurance, and telecoms. Cifas protects businesses and individuals from fraud through the sharing of data and intelligence sharing between the private, public and third sectors. It helps organisations prevent more than £2.1 billion in fraud losses each year.

Cifas has a range of best-in-class products and services to help organisations tackle insider fraud, including Vision which supports organisations in managing employee risk and monitors behavioural changes in real time, and Insider Threat Protect which helps target internal risks through data, intelligence, and learning. Additionally, its Cifas Fraud and Cyber Academy courses and the Digital Learning programme empower workforces with critical fraud prevention skills – adding a vital layer of protection.

About Us

Beruku is a specialist advisory and training firm focused on identity, personal data, and digital trust. Our team includes experts in digital identity, biometrics, cyber security, digital forensics and identity and document fraud. We have worked across both the public and private sector in policy development, commercial leadership, training and consulting roles.

Beruku is also a co-founder of Ingenium Biometric Laboratories, which is a testing, research and innovation laboratory. Ingenium helps clients test and trust identity and biometric technology, testing the performance and security of products so customers can use them with confidence in their digital and business transformation initiatives. Ingenium is also the UK's independent biometrics laboratory for the National Protective Security Authority (NPSA) and critical national infrastructure.

Fullbrook Strategies offers strategic counsel to governments and businesses around the world. Our team of experts is dedicated to cutting through the complexities of today's challenges, ensuring that your organization achieves the outcomes it needs. We prioritize results over process, delivering strategies that truly make a difference.

With expertise in strategy, research, communications, campaigning, and media management, we are your trusted partner for bespoke solutions. We possess the knowledge, relationships, and experience to tackle any global challenge, empowering individuals, governments, and companies to thrive.

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 Institute's other industry leading guidance.