tiaa.

Certified B Corporation
Learn more at bcorp.com



Issue 10

Fraud Stop

Fraudsters
Cases in Court

Fraud Spotlight
Expense Claims and Invoice Fraud

Artificial Intelligence
Risks in Recruitment

Introduction

Fraud is deception carried out for personal gain, usually for money, but can also involve the abuse of a position of trust.

The National Crime Agency website states that fraud remains a significant problem for the UK and remains the most prevalent crime against individuals in England and Wales, with the potential for causing immense financial, psychological and emotional harm.

As well as individuals, all organisations are at risk of fraud, and our experience shows that they will be targeted where key control weaknesses are identified.

Everyone has a part to play in fighting fraud. Being aware of the risk and remaining vigilant are the most important first steps, followed by knowing how to report fraud.

This edition of Fraud Stop includes recent fraud cases in court, fraud spotlights on expense claims and invoice fraud, artificial intelligence fraud risks in the recruitment process and how vulnerable people can be open to financial abuse.

Jailed academy finance boss banned from running schools after 200K fraud

An academy trust finance boss who stole £200,000 from a sixth form academy and falsified a DBS check to cover up a previous police investigation had been banned from running schools.

The fraudster was jailed after defrauding the academy between 2018 and 2021 while working as its chief financial officer.

The court was told that the stolen cash could have paid for two teachers, mental health support for vulnerable students and hardship funds.

He was jailed for 32 months in April 2025 after pleading guilty to fraud by abuse of position, fraud by false representation and concealing, disguising, converting, transferring or removing criminal property. The government has now banned him from any further role running independent schools in a decision published in August 2026.

In late 2021, the school was contacted by a whistleblower about his previous employment, which included an article regarding an investigation into financial irregularities at a community college where he had previously worked.

Although no charges were brought against him, further enquiries made by the academy trust identified payments made by him that were wholly unaccounted for, including the creation of false invoices, false journal entries and fraudulent payments, some of which were transferred to a nominated account in Nigeria.

In respect of the fake DBS check, it was established that information pertaining to a previous police case had been deliberately removed from the emailed DBS in an attempt to mislead the academy and withhold information.

Full article at: Finance boss faked DBS and defrauded academy of £200k

Covid loan fraudster who claimed 30K sentenced

The BBC reported in June 2026 that a man who fraudulently claimed £30,000 in Covid Bounce Back loans during the pandemic had been given a two-year suspended jail term after pleading guilty to fraud and money laundering at crown court.

The Covid Bounce Back Loans were a government scheme set up to support small and medium sized businesses affected by the pandemic.

The Insolvency Service who investigated the matter said that the fraudster inflated the turnover of a company he set up to find agency work as a bus driver to £60,000. He also applied for two separate loans in 2020, when businesses were only entitled to one. The investigation uncovered that his business had set up a new bank account with the sole purpose of applying for a Bounce Bank Loan. Both loans were transferred out of his business accounts on the day they were received, with none of the money used legitimately,

He was disqualified as a company director for 10 years; ordered to complete 150 hours of unpaid work and was also told he must complete 20 days of rehabilitation activity.

Full article at: Wolverhampton Covid loan fraudster who claimed £30k sentenced - BBC News



PA stole 87K in expense claim fraud

A personal assistant (PA) for a leading health and beauty retailer stole more than £87,000 from her employer in an expense fraud to fund her cocaine addiction, as reported by the BBC in June 2026.

The fraudster who worked as a PA for four managing directors duplicated expense receipts after a new system was installed in July 2022.

An internal audit found that she put through the expenses on behalf of two of the directors and had used their login details to approve payments to herself.

At Crown Court, she was sentenced to 21 months in prison, suspended for 18 months, and given 250 hours of unpaid work to complete. The court heard it was company policy for directors to approve expenses; however, the PA was in a position of trust and did so herself.

When investigated, it was found that she would input expenses providing her own bank details as the recipient and then log on to a manager's account to approve them. In total, £87,650.51 was stolen from her employer.

The fraudster was sacked by her employer and her offences reported to police following the internal audit.

She had provided no comment in interview when she was arrested in 2024 but later pleaded guilty to fraud by abuse of position and was sentenced to 21 months in prison, suspended for 18 months and given 250 hours of unpaid work to complete.

Full article at: Boots PA stole thousands in expense fraud - BBC News

Benefits cheat caught at gym classes

The BBC reported in May 2026 that a woman who claimed thousands of pounds in benefits saying arthritis left her on crutches and struggling to leave home, has been jailed after CCTV showed her taking part in classes at a gym. The fraudster was also a member of a running club and had completed a 10km run in just over an hour. She had told the Department for Work and Pensions (DWP) that severe rheumatoid arthritis in every joint and a slipped disc in her back had left her housebound.

She was jailed for seven months after the DWP acted on a tip-off, with investigators establishing she regularly attended a range of gym classes.

The DWP accused her of falsely claiming £42,013 in Personal Independence Payment (PIP) but accepted a guilty plea to a sum of £25,244.

She had claimed her arthritis was a lifelong condition that would progressively get worse and said she could not walk for more than five minutes without the crutches. She also told the DWP she needed help with washing, bathing, dressing, preparing meals and eating and drinking.

Full article at: Housebound' benefits cheat caught at gym classes - BBC News

Fraud Spotlight

Expenses and Allowances Fraud

Expenses and allowances fraud occurs when employees submit claims that are inflated or false so they can obtain additional payments at the expense of their employer. It includes any behaviour that falls outside of the organisation's policy for claiming expenses and allowances, where there is a clear intention to gain personally through false claims.

Common examples include inflating mileage claims or colleagues saying they travelled separately when they travelled together.

Frauds are typically enabled by poor procedures and weak controls, so having a robust expense policy, clear procedures, routine monitoring, along with the active promotion of an anti-fraud culture can help organisations reduce the risk of fraud.

What are the red flags?

- Claims that are vague, lack receipts or where the receipts are unclear or undated
- Unusual claims such as trips or meetings that do not seem to fit with normal business activities
- Individuals making duplicate claims or frequent errors in expense submissions
- Outliers such as team members who consistently claim higher expenses and allowances than others
- Staff members approving their own expense claims or approving each other's claims (for example, managers at the same grade)
- Falsified or unrecognisable authorisation signatures

How can it be prevented?

- Expense policies that clearly set out expectations and parameters for all types of expenses and allowances claims
- Training on the expenses and allowances policy, with reference to the organisation's disciplinary and anti-fraud policies for breaching policy
- Establish a time limit for submitting claims
- A requirement to retain original documents such as receipts
- Include a declaration on expense claims that the claim is accurate and complete, making the consequences for fraudulent claims clear
- Monitor for unusual activity and inconsistencies
- Conduct regular audits
- Consider electronic systems/expenses management software. These systems can track expenses in real time, including corporate credit card transactions and e-receipt data. They can also be linked to mobile expense apps that provide instant expenses data and GPS information to corroborate travel claims.

Contact Tiaa if you would like to fraud-proof your expense claim policies and processes - see the end of this newsletter for contact details.



Fraud Spotlight

Trusted family members, friends, and carers steal £51 million from pensioners

Report Fraud is run by the City of London Police and is the place to inform the police about fraud and economic crime.

The organisation has recently reported that older and vulnerable people are seeing millions of pounds stolen from them with the fraud committed by those closest to them and is encouraging anyone who supports an elderly relative, acts under a power of attorney, is involved in administering an estate, or works within the care sector to remain vigilant for signs of financial abuse.

Data from Report Fraud reveals that criminals stole £93.8 million through fraud by abuse of position during the 2025/26 financial year, with people aged 70 and over accounting for more than £51 million of those losses. This type of fraud occurs when someone exploits a position of responsibility, authority, or trust to access and steal a victim's money, assets or property without lawful authority. Offenders are often family members, friends, carers, employees, or individuals entrusted to manage another person's finances or affairs.

The City of London Police has issued the following guidance:

- Review financial statements: check financial statements regularly for any unauthorised transactions. If anything appears suspicious, contact the bank as soon as possible.
- Watch for warning signs: be alert to unpaid bills, missing possessions, or unexpected changes to a will or bank account, as these may be indicators of financial abuse.

What to do if you are a victim of fraud by abuse of position:

- Tell your bank or card provider: if you notice any financial transactions made without lawful authority, notify your bank or card provider as soon as possible.
- Act quickly if something feels wrong: you can raise a safeguarding concern with your local authority's adult social care team. If a solicitor or deputy may be misusing their role, you can report your concerns to the Office of the Public Guardian.

The full article and how to report these types of concerns is at: Trusted family members, friends, and carers stole £51 million from pensioners, City of London Police reveals - Report Fraud

Artificial Intelligence Risks in Recruitment

NHS Employers has identified that the use of Artificial Intelligence (AI) tools is an emerging risk in recruitment, enabling candidates to misrepresent their qualifications, experience, or identity through the use of artificial intelligence tools. Examples include AI-generated CVs, fabricated employment histories, manipulated interview responses, and the use of deepfake technology during virtual interviews. These practices can undermine the integrity of recruitment processes, increase the risk of employing unsuitable candidates, and expose organisations to financial, operational, and reputational risks. Employers should strengthen screening and verification processes to ensure recruitment decisions are based on genuine skills, experience, and identity.

Organisations should consider:

Does the Recruitment Policy (or equivalent) include content regarding the "Acceptable Use of AI by candidates"

Be clear in the policy that the organisation recognises that candidates may use AI tools to improve spelling, grammar, formatting, and presentation of application materials. Candidates must ensure that:

- Information provided remains accurate and truthful.
- Examples, experience, and qualifications are genuine.
- Assessment responses represent their own knowledge and abilities unless otherwise permitted.

Undisclosed AI use that materially misrepresents capability or suitability may be treated as recruitment fraud.

The policy should also be clear that AI tools should not be used by candidates during online interviews





Do application forms require candidates to make a declaration on whether AI tools have been used to complete the application? If AI has been used, is there a further declaration that information provided remains accurate and that examples, experience and qualifications are genuine?

It is fair to say that a large percentage of candidates will use AI – and it can be acceptable as detailed above. Transparency is key and employers should not be intolerant and adapt to its presence.

Be mindful that some candidates with disabilities such as dyslexia will find AI a useful tool.

Balancing AI assistance with personalisation to convey individual skills, knowledge and experience is key to leveraging AI benefits without compromising integrity.

During online interviews is there an initial question to the candidate to confirm via a verbal declaration that AI is not being used during the interview?

Real-time AI tools provide prompts or suggested answers during virtual interviews and candidates can appear more knowledgeable or competent than they are.

Consider a standard question to be asked at the outset of an online interview – is the candidate using any AI tools?

Are interviewers trained to spot red flags during online interviews that indicate the candidate is using AI?

Red flags include but are not limited to:

- Is the camera on?
- Do they have a second device/screen?
- Can you see their hands?
- Are they wearing an earpiece?
- Is the candidate engaged or distracted?
- Does the candidate mute and pause before answering?

Consider face to face interviews for senior or high-risk roles.

For further guidance: Guidance on the use of artificial intelligence in candidate applications | NHS Employers

Invoice Fraud

The National Crime Agency (NCA) has published useful guidance on invoice fraud, which can be the costliest form of financial crime affecting organisations. The NCA reports that the Education sector is a consistent target for invoice fraudsters, although any sector is at risk.

Invoice Fraud happens when criminals deceive you into paying a fake invoice or diverting a genuine payment into their own bank account. Fraudsters can impersonate suppliers, intercept emails or send convincing invoices to generate immediate payments into their own accounts. Remember invoice fraud is a sign of the sophisticated tactics of criminals, not a sign of negligence.

Key prevention advice:

CHECK for any changes to invoice details, bank details or if you are being pressed for an urgent payment

VERIFY by calling the genuine supplier on a previously used phone number before you transfer money, as emails can be intercepted or diverted

NEVER transfer money until you are satisfied all details are correct

The full NCA guidance on invoice fraud and what to do if you have been a victim can be found at: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/787-invoice-fraud-infosheet

What to do if ou Suspect You Have Been a Victim of a Scam

If you receive a call and suspect it to be fraudulent, hang up. If you are suspicious about an email, forward it to:

- report@phishing.gov.uk
- If you are suspicious about a text message, forward it to the number 7726, which is free-of-charge.

If you believe you are the victim of a fraud, please report this to Report Fraud as soon as possible by visiting https://www.reportfraud.police.uk/ or calling 0300 123 2040. Contact your bank immediately if you think you may have lost money.



Everyone has a part to play in fighting fraud. If you suspect any fraud, bribery or corruption against your organisation, contact your Anti-Crime Specialist.

If you would like investigation support or assistance on completing fraud risk work including reviewing fraud prevention procedures for the failure to prevent fraud offence, completion of a fraud risk assessment or fraud awareness training, contact Tiaa's Director of Governance, Risk & Compliance, Nick MacBeath at:
Email: nick.macbeath@tiaa.co.uk

Certified B Corporation
Learn more at bcorp.com

tiaa.

Disclaimer:
The content of this document is intended to give general information only. Its contents should not, therefore, be regarded as constituting specific advice, and should not be relied on as such. No specific action should be taken without seeking appropriate professional advice.

tiaa.co.uk
T: 0845 300 3333