



Issue 9

Fraud Stop

Charity Fraudsters

Cases in Court

Artificial Intelligence

Risks in Recruitment

Insider Fraud

Building your charity's defence
against insider fraud

Introduction

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

Every charity, NGO and not-for-profit is susceptible to fraud and cybercrime by criminals exploiting the current global crisis.

Charities need to be aware of the risks and take steps to keep their money, people and data safe, and Tiaa is proud to support Charity Fraud Awareness Week.

From a Tiaa perspective, all organisations are at risk of fraud, and our experience shows that they will be targeted where key control weaknesses are identified. At times when organisations have unfilled vacancies, where positions are filled by temporary employees, or where existing employees may be struggling with financial or emotional wellbeing, fraud awareness and vigilance is even more important to ensure your employees and leaders are aware of the risks and can take steps to keep your money, people and data safe.

This edition of Fraud Stop includes a round-up of court cases in the charity sector, artificial intelligence fraud risks in recruitment and building your charity's defence against insider fraud.

Fraudster who stole Gift Aid worth £700k is jailed

The BBC reported in June 2026 that a fraudster had been jailed after faking hundreds of charitable donations to steal more than £700,000 from the public purse.

The individual ran a sophisticated Gift Aid scam which led to huge payouts made to him by HMRC between March 2020 and May 2021. The money was used to pay off significant personal and family debts, including mortgages on several homes.

He was jailed for four years and eight months at Crown Court, having admitted revenue fraud and three offences of transferring criminal property.

The fraudster had used a community amateur sports club that he had set up as a front for his fraudulent activities, and he made 60 false Gift Aid claims to HMRC totalling more than £1m, of which £708,750 was paid out.

Gift Aid is a government scheme that allows charities and community amateur sports clubs to reclaim tax on donations made by UK taxpayers.

However, this individual lied about his donors. The false claims submitted by him stated 716 individuals had donated between £5,000 and £10,000 to the club.

HMRC began its investigation in 2021 and found many of the donors had been duped about a cryptocurrency mining scheme that he had promoted.

Investigators have managed to forfeit £215,000 from a bank account he owned - and have traced a further £485,750 to his personal account. Confiscation proceedings are ongoing under the Proceeds of Crime Act.

Full article at: [Chelmsford fraudster who stole Gift Aid worth £700k is jailed - BBC News](#)



Financial adviser jailed after £2m fraud spree

In a second case reported by the BBC in June 2026, a financial adviser defrauded a charity, his friends, neighbours and his clients out of almost £2m by telling people he needed a loan to pay for a divorce or inheritance payment.

The financial adviser defrauded 34 people, a charitable trust he was the chairperson of, as well as the residents' association of an estate where he was living.

The fraudster falsely promised people he would pay them back within a few days, which he would confirm in writing by email or a signed document.

He was jailed for eleven years at Crown Court in June 2026, after pleading guilty to almost 40 charges of fraud at a hearing the previous September.

His spree started in November 2022 when he approached people he knew to ask for a short-term loan. The qualified financial adviser then began approaching his clients, using his knowledge to secure loans.

He also created false documents, again to obtain further funds, eventually defrauding 34 people and securing £1,754,736.68 from them.

The fraudster was also the chair of a well-known charitable trust and had access to the accounts.

He duped trustees into believing £206,500 would be used for the charity - instead paying the money into his own account, according to the police investigation.

In addition to this, he also took money from a residents' association in an estate where he was living and transferred £1,245 into his own account.

By the end of May 2023, he had stolen approximately £1,962,481.68, from a total of 36 victims.

The investigation established that he had been investing the money he had stolen into his crypto wallet.

After being arrested on suspicion of fraud and money laundering offences, he subsequently admitted to 34 counts of fraud by false representation, three charges of making or supplying an article for use in fraud and two counts of fraud by abuse of position.

Full article at: [Droitwich financial adviser jailed after £2m fraud spree - BBC News](#)

Charity boss charged over missing trip funds

In August 2026 it was reported by the BBC that a senior scouts boss had been charged with fraud after about £200,000 raised towards a children's summer trip to North America went missing.

More than 100 scouts saw their two-week trip to Canada cancelled when the money was removed from a charity account.

Police said the scouts boss had been charged with fraud by abuse of position and related to a report of theft from the Scouts Association earlier in 2026.

The Canada visit included 100 children and 27 volunteers and parents and scouts had been fundraising since the start of last year, with the excursion costing £2,750 per child.

The trip was set to take place in the summer before it was cancelled.

The individual was a scouts' commissioner, a role he held from 2017 until earlier this year.

The fraudster pleaded guilty to fraud in October 2026, where he received a 32 month prison sentence, suspended for two years and was instructed to complete 220 hours of unpaid work.

Full article at: [Worcester Scouts boss charged with fraud after £200k goes missing - BBC News](#)

Jail sentence for £200K charity fraud

In August 2026 the BBC reported that an accountant had been convicted of defrauding a charity out of £200,000 and had been jailed for three years and nine months.

The fraudster siphoned off the money over a nine-year period while she was treasurer of an Agricultural Association.

The court heard that her paid role between 1996 and 2018 was to manage the accounts by paying bills, oversee invoices and chase payments, with the offences relating to the period 2009 to 2018.

Concerns were raised when suppliers were contacted and confirmed they had never received payments they were owed. The investigation established that she forged signatures and made it appear she paid companies for work which was not required as she used some of the money to pay off her own credit card bills and made other purchases.

The individual, who also had her own accountancy and bookkeeping business, was able to bypass limited checks and balances to commit the prolonged fraud which only came to light after a hacking incident.

Full article at: [Woman who defrauded £200k from charity jailed for four years - BBC News](#)





Former charity finance employee sentenced for £92K theft

The City of London Police reported in September 2026 that a former finance employee who diverted almost £92,000 intended for a leading breast cancer charity into his own bank account and spent the money on personal debts, luxury purchases and travel had been sentenced.

The fraudster appeared at the Royal Courts of Justice on 1st September 2026 where he was sentenced to two years and six months in prison after pleading guilty to fraud and money laundering offences.

The court heard that he exploited his position within the charity's finance team to intercept a refund payment worth £91,966.72 that should have been returned to the charity.

The refund payment from a hospital was due to the charity. However, the fraudster used his work email account to send altered bank details to the hospital on the charity's headed paper. The bank account supplied belonged to him.

As a result, the refund payment of £91,966.72 was transferred into his own personal bank account.

Within weeks of receiving the funds, he embarked on a spending spree, using the stolen money to pay off personal debts, make cash withdrawals, fund wedding and honeymoon expenses, purchase luxury items and transfer money to family members.

Evidence recovered during the investigation showed he was heavily in debt before receiving the money.

After suspicious activity was detected, his bank froze and later closed his bank account. At the point it was frozen, £42,866.25 remained in the account and was subsequently recovered.

Full article at: [Former charity finance employee sentenced for stealing nearly £92,000 from breast cancer charity | City of London Police](#)

Building your charity's defence against insider fraud

Insider fraud is when someone exploits their role or occupation for personal gain by deliberately misusing the organisation's assets and resources. It often includes the abuse of trust and can be committed by a trustee, an employee or a volunteer.

The risks are significantly increased by inadequate controls, excessive reliance on trust and individual responsibility, and a lack of effort devoted to challenging and overseeing key activities.

Consider the following checklist to build your charity's defences:

- Is there a workplace culture in which fraud is never acceptable, and everyone knows it? An essential part of preventing fraud is to have the right 'tone at the top'. It is much easier to create a good counter fraud culture when staff are guided and supported by trustees and senior managers.
- Is there an effective anti-fraud, bribery and corruption policy in place and is the policy communicated effectively to all staff and volunteers at the point of recruitment and at regular intervals thereafter?
- Is there a response plan for when an insider fraud does happen? This may be separate or included within the anti-fraud, bribery and corruption policy. A response plan should provide a clear process for detecting, investigating, containing, reporting and recovering from fraud incidents. The purpose is to minimise financial loss, protect the organisation, preserve evidence, and meet legal and regulatory obligations.
- Is a whistleblowing or raising concern policy promoted and supported widely within the organisation? Making it easy for your staff and volunteers to raise concerns can be very helpful in identifying wrongdoing, but only if people really trust the mechanism and process. It's important to remove as many barriers to speaking up as possible.
- Are there standard operating procedures that reduce risk and are being followed? For example, are there financial procedures that include segregation of duties and authority and approval limits?
- Is there robust pre-employment screening of new recruits and in-service checks for established employees? As a minimum consider eligibility to work, identity, references/work history, qualifications and whether a DBS check is required. Always ask to see original documents.
- Are there registers of gifts, hospitality and conflicts of interest and are they transparent and reviewed regularly? Is there a conflict of interest policy and is this communicated effectively to staff? It is usual to require any person joining the board of trustees to declare any conflicts of interest, as well as requiring them to confirm at the start of each trustee meeting that they do not have any conflicts of interest. Again, it is usual to require any employees to declare conflicts of interest as part of joining the charity. Depending on the seniority and role of the employee, it may also be prudent to require them to make a declaration on an annual basis. It is not always the most senior roles which carry the greatest risk from any conflict of interest. Anyone who is involved in decision-making for the charity, for example in procurement, may warrant a more rigorous approach.
- Is mandatory anti-fraud and corruption training provided to new staff and periodically thereafter? Training helps employees recognise, prevent and respond to fraud risks before they cause financial, operational or reputational damage.

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.

Top 6 fraud risk areas for charities

Our work with charities has identified six common areas where organisations may be vulnerable to fraud:

Lack of a Fraud, Bribery and Corruption Policy

Without clear policies and reporting procedures, fraud risks may go undetected and unmanaged.

Insufficient Anti-Bribery Controls

Charities without robust anti-bribery measures may be exposed to legal, financial and reputational risks.

Limited Awareness of Reporting Procedures

Staff, volunteers and contractors should know how to report concerns about fraud, bribery or corruption.

Failure to Benchmark Against Charity Commission Expectations

Charities should assess their arrangements against the guidance set out by the Charity Commission on tackling fraud and financial crime.

Lack of Board-Level Oversight

Fraud, bribery and corruption should be regularly discussed at board or committee level to promote a strong anti-fraud culture and ensure risks are properly monitored.

Failure to Prevent Fraud Offence

Organisations should be aware of the new 'failure to prevent fraud' offence introduced under the Economic Crime and Corporate Transparency Act (ECCTA) 2023, which came into effect on 1 September 2025.

What to do if You 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

