

Preventing fraud

Overview

- [What is fraud?](#)
- [Types of fraud](#)
- [Charity specific fraud](#)
- [Steps to prevent fraud](#)
- [How to report fraud](#)
- [What action can be taken](#)
- [Useful resources](#)
- [Disclaimer](#)

What is fraud?



Fraud means deliberately misusing someone else's resources for private gain. Fraud may be against an individual or an organisation. It can happen online, in person, or through paperwork and can range in amount from a few pounds stolen from petty cash to thousands of pounds taken through grant fraud.

If your organisation has suffered fraud, you are not alone. **The National Crime Agency & National Audit Office** suggests that the charity sector is affected by billions of pounds of losses from fraud every year.

Fraud is especially hard for charities because it can damage a charity's reputation, and this can result in further loss of public support and funding. The effects of fraud not only impact the organisation, its staff, and volunteers, but ultimately result in lost, or reduced, services for the public.

Types of fraud

There are two main types of fraud **insider fraud** and **external fraud**.

Insider fraud

Common examples of insider fraud include:

- Theft of cash assets
- Bribes paid to staff by suppliers or beneficiaries
- Supplies sold for personal gain
- Unauthorised personal use of assets (e.g. telephones, vehicles)
- Staff or trustees being paid inflated expenses (supported by false receipts)
- The same project being funded by two different donors
- Pay or other resources given to ghost staff or beneficiaries, who do not really exist

External Fraud

Common examples of outsider fraud include:

- IT fraud e.g. ransomware, phishing emails etc.
- CEO fraud
- Phoney fundraisers using the charity's name
- Shoplifting
- Authorised push-payment scams

Some of these newer terms may not be familiar to you:

Ransomware

Ransomware is when a hacker gains access and transfers personal data held by the organisation and locks the data until a payment is made to release it.

Phishing emails

Phishing emails invite a person to click on a link and enter details that will allow fraud to occur.

Authorised push-payment scams

Authorised push-payment scams involve manipulating people into making real-time payments, often using psychological manipulation to persuade the person the payment is urgent.

CEO fraud

CEO fraud, also known as Business Email Compromise (BEC), is a scam in which high level executives (also known as C-level executives) are impersonated, giving employees urgent and confidential orders to make financial transactions in a way that does not follow the company's standard procedures.

Cybercriminals attempt to build trust in their victims by using information that is publicly available online, thus making any topic seem credible.

Charity specific fraud

Charity scams range from someone posing as a street fundraiser for an existing charity and then pocketing the funds raised, to someone setting up a completely bogus charity to secure funds for themselves.

It is also fraudulent to apply for grants for duplicate funding, for the same use, from two sources.

Emerging risks such as deepfake scams and AI-generated phishing may also pose threats to voluntary organisations.

Steps to prevent fraud

Having the right policies and procedures in place protects both the organisation and its employees/volunteers.

The most important thing that organisations can do to combat fraud is to recognise that it happens. It is often carried out by a member of staff or a volunteer – often by people who have been with the organisation for a number of years and are seen as trustworthy. It is important to realise that given the wrong circumstances, and the right opportunity, anyone can succumb to the temptation to commit fraud.

Having the right policies and procedures in place protects both the organisation and its employees/volunteers.

Every organisation should have an anti-fraud policy setting out how to recognise and respond to fraud. This should include definitions of fraud, how the charity is working to prevent fraud, and how to report concerns both within the organisation and to external organisations e.g. the police. This should include information on whistleblowing. The policy should include a requirement for fraud to be investigated internally, whether or not the suspicion has been reported to the police or **Charity Commission**.

To protect against the opportunity for fraud involves a number of actions:

- Assess the potential risks of fraud within your organisation and consider implementing specific additional security measures, or seeking professional advice, where appropriate
- Know your staff and volunteers so that you can support them and be aware if they are under financial, or other, pressures
- Ensure you have set up financial controls including measures to ensure dual control, segregation of tasks and data protection (see our training module on Setting up a financial system/financial controls)
- Regularly monitor the work of your staff and volunteers
- Encourage everyone to speak out if they have concerns
- Train your staff to understand the dangers and potential impact of fraud, as well as recognising the signs of fraud e.g. common signs of shoplifting, emails with incorrect address details etc.
- Ensure passwords are complex (having an agreed minimum number of letters and involving numbers and symbols) and are not shared or written down
- Add two-factor authentication and phishing simulation training to cyber protection.
- Use antivirus protection and a firewall
- Install software updates promptly

- Consider creating an information asset register stating what information is held, and for what purposes, so you can assess the risks and consequences of loss or theft
- Back up computer data regularly

To prevent external fraud organisations should make sure they use a secure firewall, insist on strong, and regularly varied, passwords and consider using two-factor authentication as well as encryption.

Organisations should consider recording incidents and near misses in a Fraud Register to identify patterns and improve controls.”

“This is good practice regardless of the size or legal form of the charity.

How to report fraud

The **Charity Commission** requires charities to report serious incidents. If a serious incident takes place within your charity, it is important that there is prompt, full and frank disclosure to the Commission.

You need to report what happened and, importantly, let the Commission know how you are dealing with it, even if you have also reported it to the police, donors, or another regulator.

Reporting to the **Charity Commission** is important as it shows the trustees are taking appropriate action and allows the **Charity Commission** to offer appropriate advice. It also means the **Charity Commission** can consider the risks to other charities and advise them appropriately.

Fraud and Theft Checklist – Charity Commission website

The Charity Commission have produced a Fraud and Theft Information Checklist to consider when reporting fraud to them.

If you’re a charity worker and report certain types of wrongdoing, this is known as ‘whistleblowing’. Your employer must not treat you unfairly at work because you blow the whistle. Workers who ‘blow the whistle’ on wrongdoing in the workplace can claim unfair dismissal if they are dismissed or victimised for doing so.

All allegations of fraud must be treated seriously and investigated as soon as possible. Internal investigations must be fair and take the time to assemble real evidence before coming to conclusions. This is a detailed and time- consuming job.

An investigation may help you understand how to avoid the same type of fraud happening again in the future. But, “extreme cases make bad laws”.

It is better to change your rules and policies after careful reflection because they will have to work for normal times, as well as extreme cases.

Organisations should seriously consider recording the details of each fraud and near misses, and the actions they take in response, in a fraud register. This is an important document for monitoring fraud and for learning how to strengthen controls in the future.

Report a Serious Incident in your Charity

Where a trustee is reporting a serious incident on behalf of the trustees they can do so following the guidance given by the Charity Commission.

What action can be taken?

A number of penalties can result from proof of fraud.

The police can take criminal proceedings, resulting in possible fines and/or imprisonment for up to 10 years.

The **Charity Commission** can remove and disqualify individuals from acting as trustees if they have been involved in dishonesty or deception. They can also advise the trustees on steps to take to better safeguard the organisation in future.

Useful resources

Protect your charity from fraud and cyber crime

UK Government

<https://www.gov.uk/guidance/protect-your-charity-from-fraud>

Protect Your Charity from Fraud and Cyber Crime provides government advice on fraud and a link to the Charity Fraud Awareness Hub.

Tackling charity fraud – prevention is better than cure

UK Government

<https://www.gov.uk/government/news/tackling-charity-fraud-new-resources>

Tackling Charity Fraud – Prevention is Better than Cure is a Charity Commission publication from the Fraud Advisory Panel which gives guidance for trustees and senior management of charities in England and Wales.

The compliance toolkit: protecting charties from harm chapter 3 fraud and financial crime

Charity Commission

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/654821/Chapter3.pdf

The small charities guide to preventing fraud

Counter Fraud Campaign

https://cfg.org.uk/userfiles/documents/CFG%20resources/CFG%20Publication/CF240_SmallCharitiesGuide.pdf

The Small Charities Guide to Preventing Fraud is a guidance document produced by the Counter Fraud Campaign

Note: You have to be a member of the CGF group to read this

Action fraud

<https://www.actionfraud.police.uk/charities>

for reporting fraud [0300 123 2040](tel:03001232040)

National cyber security centre

<https://www.ncsc.gov.uk/cyberessentials/overview>

The National Cyber Security Centre has advice and information on preventing internet fraud.

HM revenue and customs (HMRC)

Tel: [0845 010 9000](tel:08450109000)

www.hmrc.gov.uk

Charity commission for England & Wales

Tel: [0845 3000 218](tel:08453000218)

<https://www.gov.uk/government/organisations/charity-commission>

WCVA and your local CVC may also offer anti-fraud resources and guidance tailored to small voluntary organisations.

Disclaimer



Third Sector Support Wales is a network of support organisations for the whole of the third sector in Wales.

It consists of the 19 local and regional support bodies across Wales, the County Voluntary Councils (CVCs) and the national support body, Wales Council for Voluntary Action (WCVA).

For further information contact

<https://thirdsectorsupport.wales/contact/>

The information provided in this sheet is intended for guidance only. It is not a substitute for professional advice and we cannot accept any responsibility for loss occasioned as a result of any person acting or refraining from acting upon it.