tiaa FRAUD STOP

Charity Edition
Autumn 2022

Charity Fraud Awareness Week 17-21 October 2022.
#StopCharityFraud

FRAUD SMART

COURT ROUND-UP

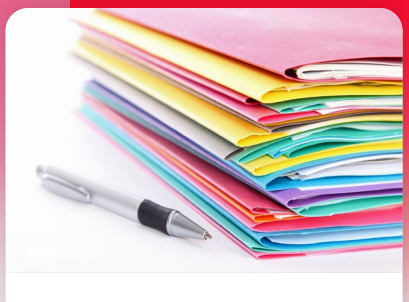
Cases that have been in court in the last year

→ SEE PAGE 2

CYBER CRIME

The growing risk post pandemic

→ SEE PAGE 3



INTERNAL CONTROLS

Anti-fraud and anti-bribery policies and Fraud Risk Assessments

→ SEE PAGE 4

Introduction

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.

Who is it for?

- Trustees, directors, board members, staff and volunteers
- Organisations that represent the interests of the sector and/or act as their voice
- Accountants, auditors and solicitors acting as professional advisors to the sector
- Regulators, law enforcers and policymakers working to safeguard the sector
- Anyone else who wants to protect the sector and the crucial work it does

Court Round-Up

In January 2022, a former employee of Autism East Midlands was jailed after they admitted spending charitable funds on holidays, concert tickets and days out. A police investigation established that the former employee had spent £145,000 of the charity's money without permission. They were entrusted with credit and debit cards as they organised residential trips for children and young people with autism, but used the cards to pay for fourteen holidays and also made fraudulent petty cash transactions. They concealed their crimes by producing fake invoices and receipts. At court they pleaded guilty to fraud by abuse of position, fraud by false representation and false accounting, and they were handed a jail sentence of three years and four months.

A former finance officer at the British Society of Echocardiography was jailed following a police investigation, after embezzling over £200,000 of the charity's money to their personal bank accounts. Their job role had included various financial functions allowing them access to the company bank accounts. Thousands had been spent on online gambling websites. The fraud unravelled when the company's bank suspected fraudulent activity. During the court hearing in February 2022, the jury heard how the former employee had a gambling addiction as well as having a depressive disorder which contributed to their actions. They pleaded guilty to fraud by abuse of position and they were sentenced to three years in prison.

In April 2022, a former charity worker who stole £187,000 from disability charity Vibrance was handed a six year jail sentence, despite claiming that they were owed the money for unpaid overtime. After being sacked, they then stole over £25,000 from a recruitment company. While working for the charity, the worker used a colleague's card and PIN to authorise payments to their own bank account and later stole tax rebate cash for workers at the recruitment company. At court, they were convicted of fraud with the jury returning unanimous guilty verdicts.

A female has been jailed for their part in a £2 million fraud against the charity Morris Curello World Evangelism. They had been involved with a male, a former charity employee who was convicted of defrauding the charity in 2017, and had received more than £800,000 from them via bank transfers and other gifts between 2013 and 2017. The female moved the criminal proceeds from one account to another following the arrest of the male. A police investigation proved that the female had benefitted from the male's illegal activity, and the female was jailed for three years in September 2021 after being found guilty of fraud by false representation.

The growing risk of cyber fraud post pandemic

There are many types of cyber dependant crimes and across the sector a significant 'triple threat' is emerging.

Ransomware attacks that target critical systems that charities rely on daily. Demands are made for payment so that systems can be brought back online. Some of these ransomware attacks are simply opening an unsolicited email or clicking on a link contained within an email, document or website.

Denial of service attacks happen when systems are flooded with traffic causing a system crash. The systems take time to recover resulting in the organisation being unable to operate. Within the charity sector this could be a donation service causing a significant reduction in income.

Insider threats are a significant risk as those working for organisations have access to valuable information. The risk increases if staff feel undervalued or are potentially put in place to deliberately access systems, obtain data, or divert payments as examples.

Source material: Be alert to the growing risk of cyber fraud post pandemic - Prevent Charity Fraud

5-Step Cyber Response

Use passwords →

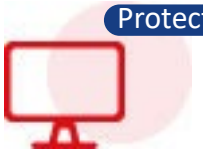
Use passwords: Switch on password protection on all devices. Consider using multifactor authentication to access devices and ensure any manufacturer's default passwords are changed. Don't use predictable passwords, and consider using password managers to avoid password overload.

Back up your data →

Back up your data: Identify your essential data and keep a backup copy of this separate from your computer. This could be on a USB stick, separate drive or on some form of cloud-based storage platform.

Protect yourself from malware →

Protect yourself from malware: Install and turn on antivirus software. Prevent your staff from downloading apps from unknown vendors or sources, and keep all of your IT equipment and software up to date by applying security patches as soon as they are available. Switch on your firewall and control how people can use external storage devices.



Protect your devices →

Protect your devices: Ensure your devices can be tracked, locked and remotely wiped if they are ever lost or stolen. Keep your device operating system and your apps up to date and do not connect to unknown wi-fi hotspots – use 3G or 4G mobile networks instead.

Avoid phishing attacks →

Avoid phishing attacks: To reduce risk, minimise the number of people who have administrator access on your network. Train your staff to spot phishing emails and tell them what to do if they have any concerns. Publicly accessible information will often be used to make phishing emails seem more plausible, so think carefully about what you post online and review this information regularly.

Source material: Cyber security - Prevent Charity Fraud
The National Cyber Security Centre has produced guidance for charities on how to improve cyber security. See Small Charity Guide - NCSC.GOV.UK for advice on backing up data, protecting your charity from malware, keeping devices safe, using passwords and avoiding phishing attacks.

Internal controls

It is vital that all charitable organisations have an effective fraud response plan in place. This should include a definitive anti-fraud policy that provides guidance on the responsibilites of staff and the Charity's expectations; a training programme for staff as well as defined reporting routes and a dedicated point of contact.

In conjunction with the above fraud controls, it is a requirement under the 2010 Bribery Act legislation that all organisations should have adequate procedures in place to prevent bribery. This includes a comprehensive gifts and hospitality policy, a robust declarations of interest procedure and an overarching anti-bribery policy.

Consider the following six principles to inform your actions:

- The action you take should be proportionate to the risks you face and the size of your business.
- Those at the top of an organisation are in the best position to ensure their organisation conducts itself with out bribery.
- Think about the bribery risks you might face given the specific context of your organisation, its activities and areas of operation.
- Knowing exactly who you are dealing with can help to protect your organisation from taking on people who might be less than trustworthy.
- Communicating your policies and procedures to volunteers, staff and partners will enhance awareness and help to deter bribery.
- The risks you face and the effectiveness of your procedures may change over time.

TIAA Anti-Crime Specialists can assist in developing robust anti-fraud and anti-bribery policies for your organisation as well as providing advice on developing a fraud and bribery risk assessment, which can assist in identifying gaps or weaknesses in controls and mitigate those risks.

If you would like advice on strengthening your anti-fraud policies and processes, contact:

Melanie Alflatt, Director - Risk and Advisory, Email: fraud@tiaa.co.uk