CHARITY COMMISSION
FOR ENGLAND AND WALES

FRAUD
ADVISORY
PANEL

# TACKLING CHARITY FRAUD
# PREVENTION IS BETTER THAN CURE

SUPPORTED BY

Crowe Clark Whitehill™

A Member of Crowe Horwath International

This guide is for trustees and senior managers of charities in England and Wales as well as their professional advisers. It summarises the main lessons and messages from the second national charity fraud conference and second national charity fraud awareness week. It also provides pointers to additional expert sources of information, support and best practice.

It should be read alongside the summary of proceedings from the first conference.

**ABOUT THE ORGANISERS**

**Charity Commission**
The Charity Commission registers and regulates charities in England and Wales. It ensures that charities meet their legal requirements and provides guidance to help them run themselves as effectively as possible while also preventing abuse (including fraud).
**gov.uk/government/organisations/charity-commission**

**Fraud Advisory Panel**
The Fraud Advisory Panel is the independent voice of the counter-fraud profession. It champions anti-fraud best practice and works to improve fraud awareness, understanding and resilience. **fraudadvisorypanel.org**

**SUPPORTED BY**

**Crowe Clark Whitehill**
Crowe Clark Whitehill is a leading provider of audit and audit-related services to charities. Its services, offered worldwide, include fraud prevention, detection and response.
**croweclarkwhitehill.co.uk**

**Building a fraud-resilient charity is a job for everyone, everywhere, and at every level.**

All trustees and managers should have the knowledge and skills to recognise the tell-tale signs of fraud and then shape an effective and proportionate response.

## WHY FRAUD PREVENTION MATTERS

There are three compelling reasons why it has never been more important for charities to remain alert to fraud risks and to maintain the kind of good housekeeping practices that can protect their operations, donors and beneficiaries.

1. **The size of the threat.** According to the Office for National Statistics there were 4.7m fraud and cybercrime incidents in the year ending September 2017.[1] For most charities it is now a question of when, not if, they are targeted. Fraud is already thought to cost the charity sector as much as £2.3bn each year.[2]

2. **An overloaded criminal justice system.** Police can no longer deal with every reported case of fraud. They might take more notice of a fraud against a charity (because of the public interest aspects) but not necessarily, especially if small sums are involved. In any case, there is no guarantee that a police investigation will recover the money lost.

3. **The importance of public trust.** Because charities are sometimes viewed as soft targets it is important that fraudsters and the general public can see that fraud is taken very seriously. That means being proactive in preventing fraud and then handling detected frauds in an open and transparent way.

As the old saying goes, prevention is better than cure. The harm fraud does goes far beyond direct financial loss to include reputational harm, the damage done to staff, donor and volunteer morale, and the management time spent investigating and reporting frauds that should have been prevented.

Every other dimension of fraud fighting – deterrence, detection, response – requires an effective culture of prevention for its foundations.

Ultimately, every charity should develop a comprehensive, joined-up understanding of the fraud-related aspects of its operating environment. Does it specialise in high risk international locations, for example, or handle lots of cash? And what about the wider cultures, procedures, practices and vulnerabilities of its beneficiaries, contractors, suppliers, funders, employees and partners? No charity is an island. Third-party weaknesses can create significant knock-on fraud vulnerabilities for the charity itself. For vulnerabilities of this kind to be properly addressed, they first have to be recognised.

1 Office for National Statistics (25 January 2018). *Overview of fraud and computer misuse statistics for England and Wales.*

2 Crowe Clark Whitehill, University of Portsmouth Centre for Counter Fraud Studies, and Experian (November 2017). *Annual fraud indicator 2017.*

### Securing board-level support for anti-fraud defences

Effective fraud prevention begins with good governance and is underpinned by good organisational culture and sound financial management. Irrespective of the size of the organisation it is vital that its leaders understand the true risks and how to mitigate them. This is part of what is meant by 'tone at the top', whereby anti-fraud measures are supported at senior level and not delegated or treated as side issues.

If leaders are seen to lack commitment to building fraud resilience the consequences can reach far beyond the immediate organisation by damaging the charity's public standing. Recent research at the University of Portsmouth concluded that the charity sector, more than any other, is at the greatest risk of reputational damage from fraud because of the widespread harm it does to trust, which in turn reduces donations, jeopardises grants, shrinks operations and hobbles delivery.

This means that board members and management alike must act as positive role models, making it clear to staff and the wider world, through the things they do as well as the things they say, that fraud will not be tolerated under any circumstances.

They should be able to give precise answers to questions like these:

- Who is responsible for the anti-fraud agenda?
- What anti-fraud measures are in place and have they been tested?
- Does the whole organisation appreciate that fraud is a genuine and ever-present danger?
- Does everyone really understand what is meant by anti-fraud measures?
- What would we do if a significant fraud was discovered?
- Who would take charge?

Making fraud 'real' for senior executives often requires a compelling case to be made, one based on published reports about actual frauds in this sector, statistics showing the true scale of losses, case studies (including incidents gathered from within their own charity) and a properly thought-through proof-of-concept argument.

It is not uncommon for a deep cultural fear of publicity to prevent organisations mounting an effective response to fraud. Here the appointment of an anti-fraud champion of appropriate seniority can pay dividends. Equipped with the right knowledge and information, they can argue strongly for swift action and complete openness at every level.

### Preventing fraud against older victims in London

City Bridge Trust (the City of London Corporation's charitable funder) is London's largest independent grant giver, making grants of £20m a year to reduce inequality and tackle disadvantage across the capital. It is currently funding a project run by Age UK and Action Fraud to provide better protection and support to older Londoners. The aim is to help them feel safer, more secure and more confident by raising their awareness of frauds and how to report them. The Age UK network (starting with four London boroughs) will be used to spread the word about how people can avoid becoming victims or repeat victims.

Older people are often among the most vulnerable in society. Age UK estimates that 500,000 of them have lost all or some of their savings to fraud, with many having been defrauded more than once. Using an evidence-based model to reduce the number of older fraud victims is a really important step forward. Once the pilot schemes have been evaluated it is hoped that the project can be rolled out more widely.

## TACKLING CYBERCRIME

Cybercrime is often misunderstood and feared simply because the technical language and terminology sounds so frightening. 'Cyber-dependent' crimes are the technically-complex offences, frequently using specialist tools and techniques to cripple computer systems and steal data. Examples include ransomware, hacking, PBX/dial-through fraud (when a switchboard is hijacked and used to make expensive calls to premium rate numbers controlled by the fraudsters), and Distributed Denial-of-Service (DDoS) attacks (when an online system or website is overwhelmed by flooding it with bogus enquiries from other systems previously infected with malware).

But by far the most common cybercrimes are low-tech, 'cyber-enabled'. These are things like theft, forgery or shoplifting but which have been carried out with the help of computers or the internet. Since these offences always have a significant human component, they are also susceptible to fairly straightforward defences and remedies.

The government's cyber-essentials scheme identifies just five key security measures that should prevent a significant proportion of the most common breaches: boundary firewalls and internet gateways, secure configuration, access control, malware protection, and patch management. Through its website it also provides a range of useful free resources, including a cybersecurity checklist.

### Improving passwords

Improving your passwords is one very simple step that can mitigate or eliminate most cyber threats. Too many individuals and organisations still don't change the factory-set passwords on their devices or else use replacements that are far too easy to guess. (To be shocked by how quickly your existing passwords can be cracked, go to www.howsecureismypassword.net)

Here is one quick way to create passwords that are both hard to crack and easy to remember:

1. think of a phrase you know well;
2. take the initial letter from each word;
3. add some relevant numbers and symbols to create a password of 16 characters or more.

For example: my first born was born on DD/MM/YYYY. To create a unique password for a particular website simply add the name of the website at the beginning, like this: fapmfbwboDD/MM/YYYY.

### Seven top tips for preventing cybercrime

1. Use anti-virus software and keep it up to date.
2. Use a firewall to block unauthorised access.
3. Don't use the same password for several online accounts.
4. Don't click on links or attachments in unsolicited emails.
5. Always lock your mobile device.
6. Always install software updates.
7. And be careful what personal details you reveal on social media.

## Protecting your information

UK charities are thought to hold personal information for about three-quarters of the population. A data breach can do very significant damage to a charity's reputation, in large part because of the pain identity theft causes the donors, beneficiaries, staff and volunteers whose data has been stolen. So it is vitally important that charities know precisely what information they hold and why they hold it, and that they are confident that their information governance processes and storage systems are properly secure.

When planning their information security architecture many organisations simply focus too much on the wrong things (systems rather than people). Statistics from the Information Commissioner's Office (ICO) on the most common causes of information security breaches by charities and voluntary organisations bears this out: loss or theft of paperwork (21%); cyber incidents (19%); email/post misdirections (10%). Interestingly, charities are also twice as likely as other organisations to leak personal information by failing to use the Bcc function properly when sending emails (11%).[3]

Here are seven things every charity should do to bring its information governance regime into the 21st century and to help it adhere to the General Data Protection Regulation (GDPR).

1. **Create a robust information governance structure.** Nominate a member of the executive leadership team to act as senior information risk officer (SIRO). Create a broad information governance committee (with the SIRO as a member) that reports to the board. Arrangements of this kind are essential to building a solid senior-level understanding of where the organisation's vulnerabilities really lie.

2. **Create an information asset register.** This is how you make sure you know what you've got and why you need to protect it. Keep it simple but make sure it works. List all information assets and conduct a risk assessment for each one: who is responsible for it; where is it held; what are the threats, risks and consequences of loss or theft; what controls are being applied; what risks threaten those controls themselves; when was everything last reviewed?

3 See Information Commissioner's Office (2017). Available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/09/data-security-incident-trends-q1/

3. **Introduce a formal system for reporting data breaches**, including a framework for assessing events and conducting investigations. Again, keep it simple. Rate incidents according to severity (0 for a near miss, 4 for 'call the lawyers'), type and data affected. Record everything in a central register then analyse the data for trends. When action is needed remember to consider all three dimensions – people, systems and processes.

4. **Send regular updates and reminders to staff.** Encourage good practice using screen saver reminders ('Have you checked you are using the correct email address?') and posters.

5. **Test systems and recovery plans.** Penetration test your website and consider simulation testing to see what happens when your servers are shut down.

6. **Build a strong relationship with a trusted IT partner.** Base it on a robust contract that clearly defines their responsibilities and yours. If you don't want your sensitive information held on their servers make sure the contract says so.

7. **And stop talking about esoteric stuff** – polymorphic botnets, high altitude icon cannons – and start talking about real world risks and weaknesses and the true value of the charity's information and reputation.

### Keeping your data out of the hands of fraudsters

- Tightly control (or stop altogether) the sale or renting-out of data to third-party brokers.
- Perform due diligence on all third-party fundraisers.
- Keep your data secure at all times.
- Be aware of how valuable your data is to criminals.
- Audit your information security controls regularly.

*[Source: National Trading Standards Scams Team]*

### Understanding cyber insurance

Recent statistics point to widespread confusion about what this kind of cover actually looks like. Many businesses believe they have cyber insurance cover when in fact they do not. Even if you think you have it, best check. And even though cyber insurance might eliminate or reduce some costs, it can be expensive to buy. Carefully weigh up the costs and benefits before committing.

Organisations with cyber insurance should be able to reclaim penalties and other costs, as well as have access to a 24/7 helpline to support them through the typical post-breach stages, namely:

- **rescue** – what to do next;
- **response** – how to respond to data subjects whose data has been lost, as well as PR advice on what to say to the media and with whom to speak; and
- **restoration** – how to get the charity's reputation back on track.

### Taking action against fake fundraising websites

Fake fundraising websites often appear in the wake of a crisis or tragedy. In the first week after the Grenfell Tower fire at least 62 new Grenfell-related domain names were registered. Most were genuine but some were not. One not particularly convincing site was still good enough to deceive people emotionally caught up in the tragedy and desperate to do something to help. It was suspended and taken offline the very same day it was registered but not before people had donated £7,000 and the fraudster had withdrawn every penny in cash.

If you are planning a major fundraising event you should approach the City of London Police. They work closely with Nominet (the UK web register) to identity and stop suspicious activity. They can create a key-word alert system to flag up anything new online that appears related to your charity, then work with you to take down imposters.

## COMMON FRAUDS AND HOW TO PREVENT THEM

Charities, just like other organisations, face a raft of potential fraud threats. Among the most common are grant, banking and procurement fraud.

### Grant fraud

Grant fraud is believed to cost UK registered charities more than £160m each year.[4] And it's not always the biggest grants that carry the biggest risks. Small grants – often designed as quick and easy funding sources – are also vulnerable to attack, including by organised crime. There are three common types of grant fraud.

- **Application fraud** – the applicant organisation has been created for the sole purpose of stealing the funding and there was never any intention of delivering a project.

- **Identity fraud** – the contact named in the paperwork is unaware that an application has been made in their name. This is a growing threat for many charities, making it increasingly important that all applicants are verified.

- **Fraud by false representation** – the documents supplied to help the funder monitor use of the grant (often invoices and bank statements) are fake or doctored.

When grants are acquired and used fraudulently the money is typically moved on in a matter of weeks, sometimes days. By the end of the grant term it will certainly be long gone. This means grant schemes must be fraud-proofed from the off, with appropriate controls to assess and monitor the application, the project and the payments.

Here one size cannot fit all. The controls must match the risks and these will vary from scheme to scheme. Funding individuals, for example, carries very different risks to funding organisations. In addition, the control mechanisms themselves will need to be checked regularly to make sure they remain effective and that staff are operating them properly.

Grants should be awarded only to organisations with the capabilities to make best use of them, so it is important for funders to get to know and understand the applicant organisation, its people and projects. Verify all individual identities and formally assess the fraud risks associated with everyone listed in the application. (In 2015/16 checks of this kind helped one lottery funder avoid awarding grants worth £150,000 to fraudsters.) Check how the applicant's finances are being managed and controlled. Face-to-face meetings are especially useful here. Consider visiting their premises or offices to make sure they actually exist, to check who they are and to see what they do. Your formal checking processes should at the very least include the following.

1. **Information checks** – the information provided on the application form and supporting documentation should be checked against public sources such as the Charity Commission and Companies House as well as the charity's own records of previous applications.

2. **Risk checks** – the risks associated with a particular applicant or project should be formally assessed, essentially by identity-checking all individuals named in the application. Is each identity a real one? Is the person using it really who they say they are?

Use formal payment controls to make sure that grants are paid into the correct bank account and that the account belongs to the right organisation and is being used properly. Segregation of staff duties is a crucial part of fraud prevention so wherever possible make different teams and different individuals responsible for each of the key payment-related operations:

- uploading banking information to the grant management system;
- making any subsequent changes to that information; and
- verifying account details before any money is released.

You could also consider paying grants in instalments to avoid putting all of the funding at risk at the same time.

Once a grant has been awarded, the project itself should be monitored. How is it progressing? Is it meeting its objectives and delivering the promised outcomes? Is the grant being spent properly? Unannounced audit or compliance visits can be a useful way to check that the charity really is providing the services the grant was intended to pay for. Controls should include a formal signing of the funding's terms and conditions (by way of contract acceptance), monitoring of ongoing expenditure, and a health check at project's end. Watch out for bogus monitoring information, most often fake invoices or doctored bank statements.

4 Crowe Clark Whitehill, University of Portsmouth Centre for Counter Fraud Studies and Experian (2017). *Annual Fraud Indicator 2017.*

You could also consider making a sample of grant recipients subject to comprehensive auditing, with every relevant invoice, receipt and bank statement scrutinised.

Every funder should make a real effort to share in and learn from the insight and knowledge of fellow funders. Get plugged into the grapevine and stay alert. Make it standard practice to talk to others, to share concerns and pool intelligence and insights on how a particular sector or organisation is performing.

### Banking fraud

Social engineering techniques are commonly used in banking frauds to build up the victim's trust before persuading them to provide or confirm seemingly incidental pieces of information. Phone calls, electronic messages and written documents are all used to encourage the belief that they are being asked to participate in something secret, vital or urgent.

In a so-called 'vishing' attack the victim is called by someone pretending to be a person in authority – a senior colleague, supplier or bank staff member. They use all the right jargon, drop colleague names easily and seem to know exactly what they are talking about. As the story unfolds the fraudster may introduce a sense of urgency and begin to ask for confidential information about recent banking transactions, or to seek confirmation of information they already have. Care should always be taken to make sure such callers are legitimate.

A similar technique has a computer user called by someone claiming to work in technical support. They are persuaded to download software that enables the caller to gain remote access and steal data. Software should never be downloaded just because a caller has requested it.

It is quite common for users to accidentally download ransomware simply by clicking on a file disguised as a harmless email attachment. The malware then automatically encrypts user files and the fraudster demands a ransom (usually in bitcoin) to return the data to a usable format. Often the pressure is ramped up by a countdown clock which appears on the victim's screen. Routine backups, regularly tested, can ensure business continuity is maintained.

In CEO frauds an employee (typically quite junior and probably working in accounts) receives urgent instructions to transfer money to a third-party account. The email address (which will have been spoofed by the fraudsters) appears to belong to a senior board or staff member who is out of the office. The unconventional approach is explained by the commercial sensitivity of the transaction – only a few key people can know about it. And, of course, time is of the absolute essence.

#### Fighting CEO fraud

- Clearly communicate to staff the charity's policy on how financial transactions are requested, approved and verified.
- Encourage staff to be sceptical about 'urgent' and 'confidential' requests for money and data. Require them to seek independent confirmation before they act. Make sure everyone knows how easy it is for fraudsters to set up lookalike email addresses.
- Since even quite innocuous information can help a fraudster sound like a colleague, raise general awareness of the dangers of sharing inside information online.

Two similar frauds rely on forging changes to banking details or providing bogus invoices. They target the accounting staff normally responsible for paying genuine invoices, tricking them into changing payment details so that the money is transferred into the fraudster's account. (Importantly, even though the fraudster's bank account is unlikely to carry the correct name, a transfer will still go through if the sort code and account number relate to any live bank account.)

#### Fighting invoice fraud

- Make sure that invoices match the records and purchase orders on file before authorising payment. Carefully review bank account details, amounts being claimed and descriptions of goods or services provided.
- Confirm 'change of account' requests with the suppliers themselves, using contact details known to be genuine. Never assume that the information provided in the request itself is accurate.
- Let suppliers know when a payment has been made to them.

Fraud will not leap out and announce itself. Awareness is vital. To see fraud clearly we need to be alive to the possibility of it.

In an 'overpayment fraud' the victim is led to believe that they have mistakenly been sent too much money as payment for a service or product, or perhaps as a donation. The original payment will sometimes have been made by cheque. With an elaborate display of courtesy, distress or anger, the fraudster asks for their money back. If the payment was by cheque, the victim may agree to return the overpayment by electronic transfer before first making certain that the cheque has cleared.

Each of these examples shows that charities must have proper online banking procedures which are enforced and followed by well-trained staff. They should include things like: regular reviews of user roles and privileges; no sharing of system log-ins; dual authorisation of payments; strict payment limits; systematic disabling of unused system functionality and payment options; credentials kept securely; and, importantly, heightened vigilance during seasonal peaks in donations or trading. Finally, be wary of the amount of information about the charity and its senior staff that gets shared. Think about how it could be used by potential fraudsters.

### Procurement fraud

These are frauds arising out of the purchase of goods and services or the commissioning of projects (such as construction).[5] Among the warning signs are an inconsistent market, surprise or previously unheard of contract winners, bids based on unsustainably low prices (so-called low-balling), and plain-and-simple over-pricing. Watch out too for 'ghostly' indications of contract fraud:

- **Ghost goods** have allegedly been shipped by a foreign supplier but then never arrive. Or there might be problems with poor quality or short quantities, so regularly test both for consistency.

- **Ghost workers** are employees who don't exist or don't work the hours claimed, but who are billed for by the contractor or service provider nonetheless. Monitor attendance and actual hours worked, and audit both regularly.

- **Ghost performance** has been recorded but simply never happened. The greater the rewards for achieving targets, the greater the temptation to fiddle the data and lie about outcomes.

All these procurement risks can be reduced by following three simple principles of good practice:

1. Appoint a contract manager (or some other designated person) to take responsibility for all contracts. It is their job to make sure that every contract is read thoroughly and properly understood.

2. Verify performance under each contract and make sure that goods are delivered on time and of consistent quality.

3. Audit all procurement processes, and monitor and review the performance of anyone responsible for contract management.

Payment systems are also extremely vulnerable to fraud and abuse. Two of the most common frauds are the forging of changes to banking details (again) and subcontractors lying about whether a real invoice has already been paid.

The fraudulent altering of bank details (to redirect a payment into the fraudster's account) is increasingly common. The request to change bank details will often appear to be from a genuine contractor. Prevention requires a secure payment management system, careful verification of all deliveries, and scrupulous authentication of both the payee details originally entered into the system and any subsequent changes.

As we've already seen under banking frauds, strict segregation of duties is an important way to prevent these kinds of fraud. Invoice creation and payment authorisation should always be done by different people. Every employee involved in procurement should be required to take a block of leave each year so that someone else has a chance to look over their work and relationships.

5 Action Fraud.

## DETECTING FRAUD

The way charities communicate about fraud can also help them detect and prevent it. This is particularly true of their internal communications. Fraud will not leap out and announce itself. Awareness is vital. To see fraud clearly we need to be alive to the possibility of it. Staff (volunteer as well as paid) are often the first to notice that something isn't quite right so they should be encouraged to act as the organisation's eyes and ears. Give them the skills, tools and confidence they need to uncover problems and report them.

### Creating credible fraud reporting processes

It is much easier to identify problems early and address them promptly if you have a simple, hassle-free way for staff and volunteers to raise their concerns. Remove as many barriers to speaking up as possible; there will probably be more than you think and many will be hidden in plain sight:

- **Organisational** – are staff certain that their concerns will be responded to promptly, robustly and effectively? If they think allegations are unlikely to be taken seriously they won't risk speaking up.
- **Cultural** – do some staff find it difficult to discuss confidential matters with senior colleagues? Differences in age, tenure, status and 'style' can all get in the way.
- **Personal** – might staff who are thinking of speaking up have personal fears about hurting someone, losing their job or somehow being forced out?
- **Lack of knowledge** – are staff aware of reporting processes and how to use them? Remind them regularly.

In order for any staff reporting mechanism to be credible it must also be easy for everyone to access and operate. Do all staff have access to email? Can the intranet be operated discretely by everyone everywhere? Can everyone afford the cost of a hotline call?

Create a formal reporting policy which explains clearly how to raise a concern. Reporting forms need to be designed carefully, with simple language and layout, so that they are easy to understand and use. To promote trust they should also make it absolutely clear that the information will be treated confidentially.

Include a step-by-step guide to what happens following a report, including the possibility of onward referral to the police and regulator once internal investigations are complete. Then make sure this policy is widely distributed and properly understood.

To encourage staff to use the reporting mechanism it will need to be publicised and explained clearly. Stress (repeatedly) the importance of raising and tackling these problems for achieving the organisation's charitable aims and maintaining its financial health. Create a staff guide to explain the what, why, where, how and to whom to make a report.

Finally, designate someone to receive and process the incoming reports. They should ideally be a (fraud) risk manager or someone else with the seniority to match the responsibilities.

### Improving staff awareness and training

Staff awareness and training should be a key component of every charity's wider fraud fighting and risk management strategy. The ultimate objective is to raise awareness, change behaviour and use feedback to refine strategy. But before any of that is possible, first the differing needs of the charity's key stakeholders need to be understood.

- **Internal** – staff must be shown what is and is not acceptable behaviour, why they should care about fraud, what they can and should do to prevent, detect and report it, as well as the ways in which anyone raising a concern will be protected.
- **External** – donors, grant-givers, members, suppliers and anyone else the charity works with need to be left in no doubt that fraud is always taken very seriously.

Staff awareness of policies, controls and procedures should be tested regularly. Low levels of awareness can be tackled with training programmes focused (at least initially) on the main fraud risks. One way to do this is by using interactive awareness workshops; start them in high risk areas – which might be particular roles, projects, offices, departments, functions or processes – then roll them out more widely. Some charities make attendance mandatory; new recruits as part of their induction, annual refreshers for everyone else.

Workshops of this sort are also good for gathering staff views, sharing experiences and identifying weaknesses (in policies, systems and controls) that frontline staff tend to notice first. Use practical case study examples that everyone can relate to. Encourage open discussion. Gather feedback from participants and use it to continuously improve the training experience, in what should become an iterative process.

Information is an asset that needs protecting from loss, manipulation and theft. But it is also a window on the organisation's inner workings that can provide valuable insights about fraud vulnerabilities.

Don't be afraid to use posters, videos, quizzes, fraud facts, blogs and fake phishing email simulations – whatever engages your staff and helps get the message across. It's important that everyone understands that counter fraud policies are there to encourage, support and protect them.

More 'risk-mature' charities, or those with larger workforces, might want to take on larger scale or more complex awareness-raising initiatives. They might run their own in-house fraud awareness weeks or create and promote bespoke e-learning modules. Whatever the scale and nature of the training and awareness activity it must never be 'fit and forget'. It will need constant evaluation and re-evaluation to make sure it continues to deliver the results you need. And remember, you may have to be patient. Staff might be reluctant at first to share their thoughts, and all of this could take time to bear fruit.

### Using data mining tools and techniques

Information is an asset that needs protecting from loss, manipulation and theft. But it is also a window on the organisation's inner workings that can provide valuable insights about fraud vulnerabilities. Data mining offers new ways to analyse operational and transactional information to highlight anomalies and errors worthy of closer examination. It is typically done using commonly-available tools like spreadsheets and databases, but specialist audit software and bespoke data mining tools are also widely available.

For small charities, spreadsheets and databases can be a cost-effective way to conduct basic data mining activities but they do have their limitations. The number of records that can be imported is limited. No audit trails are created, making it hard to keep track of who did what to the data. Standard formatting settings can even corrupt some data as they are imported – for example by automatically removing the leading zero from some bank account and reference numbers.

Specialist audit software tools handle much larger volumes of data, produce audit trails and process histories, and can automatically alert the user to errors, anomalies or deceptions by highlighting category exceptions and outliers. They are designed to maintain the integrity of source data so their outputs are also easier to defend in court. Many have dashboard-style user interfaces that simplify tasks like management reporting and data visualisation.

Such sophisticated tools are usually only of interest to large organisations. They are expensive to buy (or lease), necessitate more user training and can sometimes provoke resistance from IT departments suspicious of the possible impact on core systems. Even large organisations may choose to outsource these kinds of systems, if only to control purchase and training costs. But outsourcing brings its own risks, especially when data is sent offshore and becomes hard to retrieve promptly in an emergency. Outsourcing contracts of this type must not be entered into lightly. They need to be expertly written and structured, with expert advice sought before anything is signed.

The key to successful data mining is the extent to which several standalone data sources can be turned into a single resource. Most charities could look into this without incurring the expense of specialist external help. Take payroll fraud as an example. What if a staff member contracted to work 20 hours a week was actually being paid for 37.5 hours? If the data on your payroll and HR systems can be linked or otherwise compared it becomes possible to highlight anomalies of this kind.

And then there are all the useful data generated constantly by commonplace technologies like email systems, mobile phones, and even the humble laptop and desktop PCs. Any investigation that does not consider forensic analysis of the data held on these systems is missing an important trick. And don't make the common mistake of thinking that deleted material can't be recovered. It can.

## RESPONDING TO FRAUD

One of the biggest barriers to tackling fraud can be a feeling among staff that fraudsters won't be punished so there's no point speaking up. And when budding fraudsters see little risk of sanction they are much more likely to give it a go. A weak fraud response at any one charity is also bad for the whole sector. People who leave one organisation under a cloud don't just disappear. They soon turn up somewhere else, doing much the same work and posing much the same risk. Conversely, when charities are prepared to act strongly and be open about what has happened they strengthen sector-wide prevention and deterrence by reducing fraudsters' opportunities to reoffend.

Every charity needs to be well prepared for fraud by following three simple principles:

1. act immediately to mitigate the effects (whether by using in-house or outside expertise);

2. always call law enforcement; and

3. have a clear, pre-prepared communication plan for working with the media.

In every sector far too many frauds still go unreported to law enforcement. Charities should always report fraud and cybercrime to Action Fraud (the UK's national reporting centre); it offers 24-hour support for victims of live cyber-attacks whether systems, money or data are at risk. The police can also take action against fraudulent websites (including bogus sites designed to impersonate real charities), especially if they are based in the UK.

Being on the receiving end of a cyber-attack (rather than a fraud or theft) is now a very serious matter. The General Data Protection Regulation (GDPR) greatly increases the responsibilities of data-holding organisations to protect personal data and report security breaches. It will also introduce some very significant new financial penalties for those who fail.

### Getting the Charity Commission involved

Among the Charity Commission's statutory responsibilities is making sure that trustees comply with their legal obligations. The commission understands that things can and do go wrong. But when there is serious abuse or maladministration, and matters need to be put right, trustees are expected to step up and take control of the situation. If they don't, the commission will step in and do it for them, deciding when and how to act by using a risk framework based on three questions:

1. Does the commission need to be involved?

2. If so, what is the nature and level of risk?

3. What is the most effective response in the circumstances?[6]

In low risk cases, advice and guidance may be all the trustees need. In the most serious cases a statutory inquiry may be opened.

The highest priority risks are covered by the Charity Commission's serious incident reporting regime. In 2015/16, of the 2,200 'serious incidents' reported to them, 178 were considered fraud. Just over one-third of those were 'insider frauds' – committed by trustees, staff or volunteers – and many were 'cyber-enabled'.[7] Even so, under-reporting is widespread; the commission's casework regularly uncovers serious incidents that should have been reported.

Weak governance and poor financial controls – too much trust placed in a few key individuals – are often contributory factors.[8] Examples include: poor financial controls relating to cheque signing (such as cheques countersigned in advance 'because the chair is often abroad'); limited or no segregation of financial duties; misuse of charity credit cards and staff expenses; and conflicts of interest (including contracts awarded to a trustee's own company or jobs given to family members). A recurring theme is a lack of adequate documentation to explain expenditure.

Charities should report all serious frauds to the Charity Commission (email: RSI@charitycommission.gsi.gov.uk), explaining what has happened and what's being done to deal with matters. Action Fraud should also be notified immediately.

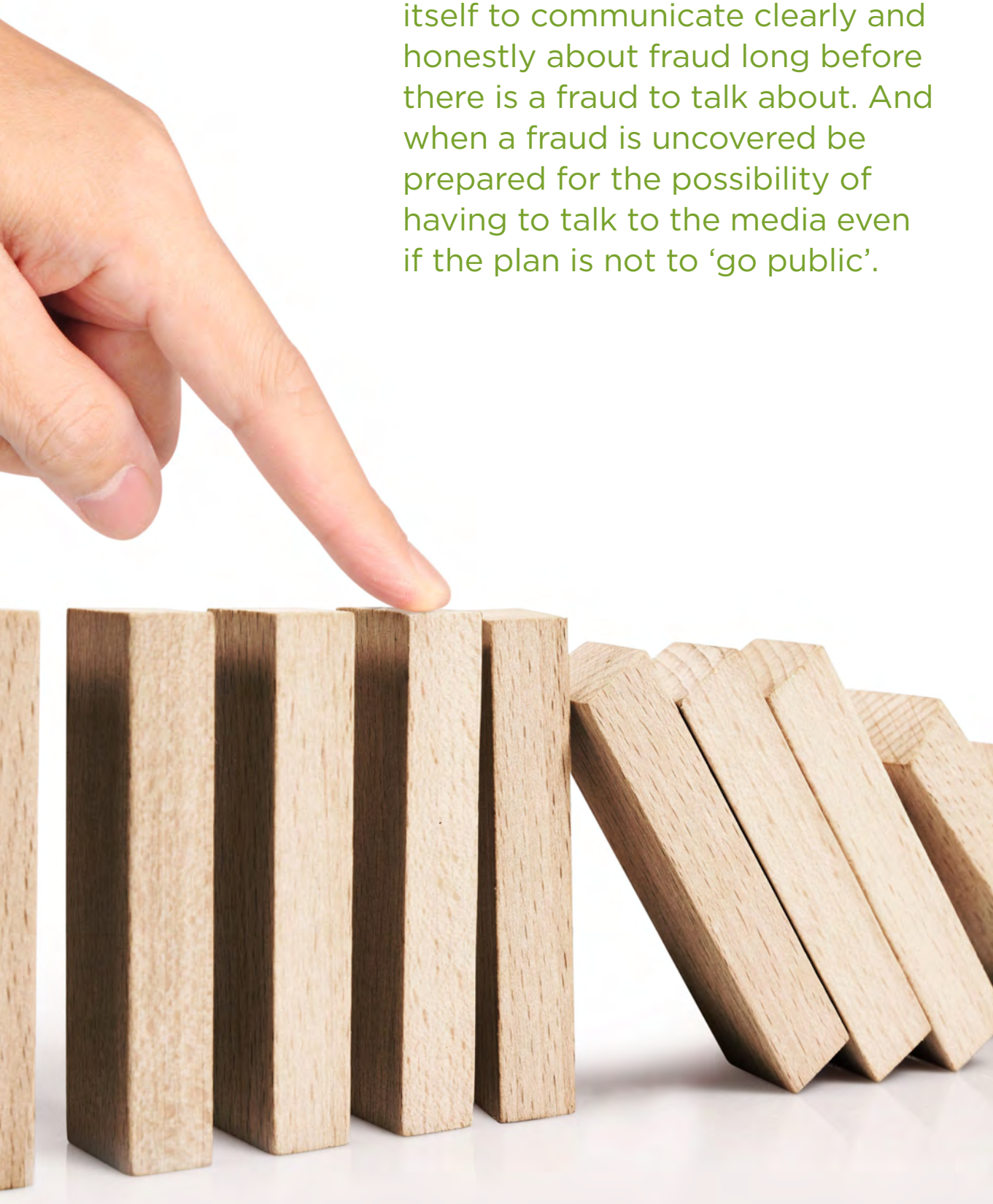
### Dealing with the media

A solid, public track record for managing money responsibly and transparently is a great defence against criticism when things do go wrong.

That said, charities face some very particular public relations challenges. News outlets often hold them to higher standards than other organisations. Even the smallest charity fraud can become a major PR headache simply

6 Charity Commission (26 February 2016). *Risk framework*.
7 Charity Commission (October 2016) *Protecting charities' funds: detecting fraud against charities*.
8 Ibid.

... every charity should prepare itself to communicate clearly and honestly about fraud long before there is a fraud to talk about. And when a fraud is uncovered be prepared for the possibility of having to talk to the media even if the plan is not to 'go public'.



because so many people (donors, fundraisers, volunteers, regulators) feel the fraud so personally. And the degree of media interest in a charity fraud story is often a function of factors over which the charity has little or no control; things like the location of its main activities, the emotional power of the personal stories or the callousness of the perpetrator.

For these reasons every charity should prepare itself to communicate clearly and honestly about fraud long before there is a fraud to talk about. And when a fraud is uncovered be prepared for the possibility of having to talk to the media even if the plan is not to 'go public'. Lots of the communications materials required in these situations can and should be readied in advance. Your fraud response plan should always include a communications protocol, properly developed and stress-tested just like everything else in it.

When fraud does strike, remember the three main principles of effective media communications.

1. **Timeliness** – generally-speaking get bad news out as soon as possible (though not before the facts are certain) and always be consistent about what is said.

2. **Completeness** – get all the bad news out in one go and show that things are being sorted out promptly.

3. **Cooperativeness** – don't stonewall journalists or try to keep them in the dark – and if law enforcement or regulators are involved, consider making joint announcements.

Stakeholders will want answers too. That means effective internal communication channels for staff, volunteers, donors and beneficiaries. They will all want to know what happened, when management first knew, and what has been done to control and recover the situation. Focus on that last question in particular, so as to be judged not on the fraud but on how the consequences were handled. Get the clean-up right and people tend to be much more forgiving about everything else.

There are certain critical moments when it is particularly important to communicate well: namely when the fraud is first discovered and later when matters are finally resolved through legal process. Prepare some clear messages and think carefully about who will speak for the organisation (the chief executive isn't always the best choice). If there are journalists with whom the charity already has a good relationship, these are the times to engage with them closely.

Lastly, when another charity is hit by fraud never comment on its woes. Instead take their misfortunes as a reminder that it's probably time to look again at your own anti-fraud processes. And be mindful that your donors may be wondering if they could be next, so they will need reassurance.

### Taking civil action in cases of low value fundraising fraud

Imagine: a local pub regular has a sponsored head shave for a cancer charity, raises a few hundred pounds, gets a mention in the local paper, but the money never reaches the charity itself. The fraud comes to light when a neighbour begins to doubt the fundraiser's good intentions and decides to check what happened to the cash. Because this scenario is not as rare as we'd like to think, some charities are now much more proactive in following up small-scale fundraising activities.

Taking action in the civil courts is now easy, inexpensive, and an effective alternative to involving the police. It also sends a positive and confidence-boosting message to donors, staff and other stakeholders that the charity is not a soft touch.

Money Claim Online (provided by HM Courts & Tribunal Service) enables claimants to start civil actions online. Once an online account has been set up the claim can be created and issued electronically. The onus is then on the defendant to contact the claimant about settlement. If they still haven't done so after 14 days the claimant can apply for a county court judgement (which can damage the defendant's credit rating). To recover money the claimant can then ask for a warrant to be issued. For claimants the service is quick, convenient and low cost. Once a claim has been issued the ball is firmly in the defendant's court and the charity can easily self-manage the whole process through the Money Claim Online homepage.

What kind of case might be suitable for this approach?

- There needs to be strong evidence of wrongdoing (such as witnesses, documents, photographs, social media posts).
- The suspect should have received at least two letters asking them to explain the missing funds.
- The second of these letters (sent by recorded delivery) should have outlined the charity's policy on pursuing fraudsters.
- But still there has been no response.

# TACKLING CHARITY FRAUD CASE STUDIES

## THE BIG LOTTERY FUND

The Big Lottery Fund is a non-departmental public body which distributes to 'good causes' 40% of the money raised by the National Lottery. In 2015/16 it made 11,700 awards totalling £583m, almost 90% of them for amounts less than £10,000.

In 2004 the Community Fund (one of the Big Lottery Fund's predecessors) discovered a fraud involving multiple grant applications. A staff member noticed similarities, including identical telephone numbers, across a number of unrelated applications. At that time the fund carried out only basic authenticity checks on applicants. New groups, with no previous application history, were being actively encouraged to apply. Further investigations found nearly 700 potentially-fraudulent applications, together worth an estimated £4.5m. The subsequent police investigation lasted six years and the nine people found guilty received prison sentences totalling 27½ years.

Criticism of the Community Fund's poor know-your-applicant safeguards prompted a comprehensive range of new measures to fraud-proof the grant scheme and prevent similar frauds in future. As well as risk-assessing applications and monitoring and controlling payments, the Big Lottery Fund now performs identity checks on the organisations applying for funds and the individuals associated with them. These include checking that every identity is a real one and that named contacts are really who they say they are. During 2015/16 these checks helped avoid potential fraud losses of £150,000.

Today one of the biggest fraud risks for the fund comes from attacks by organised crime on its small grants programmes. In 2015/16 there were 305 confirmed cases of fraud worth just under £1m in total: 238 application frauds, 35 identity frauds, and 32 frauds by false representation. To put this into perspective, 28p of every pound spent on the National Lottery goes to good causes, so each £500 fraud loss is equivalent to 1,786 unsold lottery tickets.

## BRITISH PREGNANCY ADVISORY SERVICE

The British Pregnancy Advisory Service (BPAS) takes care of almost 80,000 women each year. Its 725 staff work in 70 clinics nationwide. Income in 2015/16 was £29.1m.

In March 2012 its website was defaced by a member of the hacking collective Anonymous who claimed to have stolen about 10,000 records of website contacts and threatened to release them online. The hacker had taken six hours and 26,000 attempts to find a coding flaw to exploit; unbeknownst to BPAS their website was designed to save an html record (complete with name and phone number) every time a contact message asked BPAS staff to call back.

BPAS acted quickly to investigate the incident and inform service users. The police, ICO, Charity Commission, NHS Commissioners and other interested parties were all notified promptly. Within 24 hours the hacker had been arrested and was later sentenced to 32 months in prison. The data was recovered before it could be released.

Even though the data leakage and direct financial costs were relatively small, the real costs of the attack were much higher: bad publicity and reputational damage; anxiety for clients using a confidential service; operational disruption – the website was offline for three days; cleaning up the infected systems and getting them back up and running; and then improving all systems, processes and information governance in the light of the lessons learnt. Staff also had to repel continuing DDoS and hacking attacks, with 2,500 hacking attempts made during the subsequent five weeks. After a two-year ICO investigation BPAS was fined £250,000 (subsequently reduced to £160,000) for failing to be sufficiently aware of the risks to its systems and data.

BPAS now takes a much more robust approach to information security and IT contract management. A range of new measures have made sure that it knows exactly what personal information it holds, where it is held and for what purpose.

# Useful resources

**Action Fraud**

www.actionfraud.police.uk

**Charity Commission**

www.gov.uk/government/organisations/charity-commission

**Fraud Advisory Panel**

www.fraudadvisorypanel.org

**Get Safe Online**

www.getsafeonline.org

**HM Courts & Tribunals Service (Money Claim Online)**

www.moneyclaim.gov.uk

**HM Government Cyber Aware**

www.cyberware.gov.uk

**How Secure is my Password?**

www.howsecureismypassword.net

**Information Commissioner's Office**

www.ico.org.uk

**National Cyber Security Centre**

www.ncsc.gov.uk

**SAFERjobs**

www.safer-jobs.com

## ACKNOWLEDGEMENTS

Our sincere thanks to all the speakers who contributed to the second national charity fraud awareness week, 'Fighting Fraud Together' (23 October 2017) and second national charity fraud conference, 'Tackling fraud in the charity sector: prevention is better than cure' (28 October 2016): Mike Ashley (Charity Commission), Nick Blake (Big Lottery Fund), Robert Browell (Macmillan Cancer Support), Alan Bryce (Charity Commission), Mia Campbell (Fraud Advisory Panel), Dave Carter (British Council), Rod Clayton (Weber Shandwick), David Clarke (Fraud Advisory Panel), Martyn Croft (The Salvation Army UK), Euan Drysdale (Keegan and Pennykid Insurance Brokers Ltd), John Fernau (Fernau Solutions), Zara Fisher (Fraud Advisory Panel), Pesh Framjee (Crowe Clark Whitehill LLP), Andy Fyfe (City of London Police), Alderman Alison Gowman (City Bridge Trust), Dr Stephen Hill (Fraud Advisory Panel), Laura Hough (British Council), Diana Isiye (Oxfam GB), David Kirk (Fraud Advisory Panel), Richard Kusnierz (Haymarket Risk Management Ltd), Brian Mearns (Haymarket Risk Management Ltd), Pascale Nicholls (Amnesty International), Gerald Oppenheim (Fundraising Regulator), Claire Parris (Charity Commission), Chris Plummer (British Pregnancy Advisory Services), Neil Robertson (Charity Commission), Michelle Russell (Charity Commission), Brian Shorten (Charities Security Forum), Helen Stephenson CBE (Charity Commission), Richard Strawson (National Trading Standards), Victoria Tills, Sophie Urquhart-Scotson (RBS), and Craig Watson (RSA). Our thanks also go to Mark B Morris and Lucinda King who acted as rapporteurs.


Chartered Accountants' Hall, Moorgate Place, London EC2R 6EA, UK
T +44 (0)20 7920 8721 E info@fraudadvisorypanel.org
www.fraudadvisorypanel.org

Company Limited by Guarantee Registered in England and Wales No. 04327390
Charity Registered in England and Wales No. 1108863