CHARITY COMMISSION

FRAUD ADVISORY PANEL

Tackling fraud in the charity sector

A summary of conference proceedings

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 advisors. It highlights the main learning points from the first national conference on charity fraud held in late 2015, and provides signposts to extra sources of information, support and best practice. It concludes with a summary of top tips for preventing, detecting and responding to fraud.

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 preventing abuse (including fraud).
gov.uk/government/organisations/charity-commission

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

Published February 2016

Fraud is a serious threat to every organisation, charities included. With reported fraud increasing at an alarming rate it is vital for charities of all shapes and sizes to protect their income and assets by building strong defences.

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

'Trustees have a legal duty and responsibility under charity law to protect the funds and other property of their charity so that it can be applied for its intended beneficiaries. They must also comply with the general law (and overseas law where applicable) including in relation to the prevention of fraud, money laundering and terrorist financing.

Fraud will flourish in an environment of weak governance and poor financial management. So this means that the protection of charity funds begins with having robust financial control systems within a framework of strong and effective governance.'[1]

GOOD GOVERNANCE AND FRAUD RISK MANAGEMENT

The governing boards of not-for-profit organisations have often been criticised in the past for being *'little more than a collection of high-powered people engaged in low-level activities'*.[2] But times are changing: boards are now becoming more engaged, acting more responsibly and focusing more closely on the issues of greatest importance.

One such issue is fraud. From a governance perspective the key question is this: do you have the right people, doing the right things, at the right time, in the right parts of the organisation? And people means everyone: board and management team; staff, volunteers and supporters; partners and beneficiaries. Building a fraud-resilient charity is a job for everyone, everywhere, and at every level.

By using a fraud risk management framework we can think about this in a structured way and then put it into practice through:

- prevention (risk reduction);
- detection (fraud discovery); and
- response (corrective action).

Because some fraud will inevitability leak into any organisation you need to understand how much loss your charity is willing to accept (this is your fraud tolerance) and then put in place the systems and processes to manage that level of risk and keep exposure within acceptable limits.

1 Charity Commission (2011). *Compliance toolkit: protecting charities from harm*. Chapter 3: fraud and financial crime: summary (p1).

2 Taylor, BE, Chait, RP, and Holland, TP (1996). *The new world of the nonprofit board*. Harvard Business Review. September to October issue.

So where do you start? With the board of trustees and their management team. They must create and sustain an ethical tone right from the top. That means systematically building an ethical culture: one that demands accountability, makes clear what is and is not acceptable behaviour, encourages people to speak up while preventing reprisals, makes sure that staff (especially frontline staff) and partners are properly trained, and which ensures that the right internal controls exist and work. But it also means leading by example at all times.

High levels of trust are often a key feature of charity operations, but trust should never be used as an excuse for poor risk management. Anti-fraud principles should apply to everyone. Some of the biggest charity frauds are committed by people in positions of great trust. Senior people can enable fraud by others simply by failing to exercise proper oversight. That's why your structures of responsibility, authority and accountability are so crucial – and why there should be no exceptions to them.

Creating an ethical culture

The ethical culture of an organisation is constructed from the behavioural norms, core values and leadership styles of its members. If employees are to fully appreciate the importance of ethical behaviour, their bosses (managers at all levels) must lead by example. In practical terms that means promoting a culture of openness, transparency, dialogue and engagement.

Your charity can publicly demonstrate its commitment to ethical behaviour by formally articulating its values in a code of ethics and creating suitable structures for staff support, monitoring and accountability. In this way you can begin to change everyone's conduct and behaviour for the better by embedding values throughout the organisation.

Research has found that many employees who become aware of misconduct choose not to report it. Their reasons tell us a lot about the kind of culture we should actively avoid.

- They fear jeopardising their own position at work.
- They doubt any action will be taken.
- And they worry that their managers will see them as a troublemaker.[3]

Charities should encourage their people to speak up at work: give them confidence that their concerns will be addressed effectively in-house and they will be more active in support of anti-fraud activities and less likely to feel driven to public whistleblowing.

Using structured communications campaigns you can increase employee confidence about how, and with whom, to raise concerns. Training designed to help improve general staff understanding of fraud matters will often better equip employees to deal with their own ethical dilemmas too.

Regular employee surveys can then help you assess and monitor the health of organisational values, the effectiveness of internal policies and the level of fraud awareness among staff, as well as to provide a measure of ethical assurance for your board.

Putting the right policies and procedures in place

A comprehensive fraud strategy sets out the charity's commitment to an ethical culture and its determination to prevent, detect and deter fraud (and sometimes corruption too) and to take action whenever a fraud is suspected or discovered. This document is aimed at trustees and management. It should outline areas of greatest vulnerability (in a risk register) and describe the creation and maintenance of all your anti-fraud processes and responsibilities, including staff awareness and training.

The strategy is usually supported by a range of policies to provide a more detailed explanation of the practical approach to be taken. These will differ from one organisation to another but they should always be consistent with each other and with policies in closely-related areas such as disciplinary procedures. Keep them short, succinct and accessible. Outline the objectives of each policy. You might want to use the umbrella term 'dishonest behaviour' instead of 'fraud'. This is wider than the usual legal definitions (fraud, theft, bribery and corruption) so it might need explaining. Draw attention to the wider consequences of dishonesty (not just financial loss but things like reputational damage). And be crystal clear that your organisation will not tolerate fraud.

3 Institute of Business Ethics (2015). *Ethics at work: 2015 survey of employees: Britain.*

Anti-fraud and speak-up policies should always apply to everyone – trustees, volunteers, members, beneficiaries and delivery partners, as well as staff – so communicate them widely and publicise them prominently using mechanisms like poster campaigns in canteens and rest areas. New managers and frontline staff might need formal fraud awareness training, perhaps supported by specialist training in particular areas. And bear in mind that it may be prudent for some policies, such as those relating to investigations, to have a more restricted circulation.

Finally, you need a fraud response plan. When trouble strikes the organisation will ideally already know who will do what, and when. The conduct of inquiries will be an important part of your plan. During any fraud investigation good internal and external communication is vital. Much of this will be central reporting between the investigation team, audit teams and committee members. But if an investigation takes a long time general employee updates may also be needed, especially at times of peak activity and staff interest. Keep your colleagues in human resources in the picture too. They will have a special interest in internal fraud and certain other types of misbehaviour in case an individual's work responsibilities have been compromised. And don't forget to include guidance on the various loss recovery options available; each will have its own strengths and weaknesses in a given case.

Conducting annual fraud risk reviews

It is very important to provide stakeholders with reliable assurance that your anti-fraud policies and associated procedures are fit for purpose and working properly. To this end, every charity should assess its operational environment by conducting an annual fraud risk review and then making the findings available to its board of trustees.

Give yourself a head start by using the checklists published by the Charity Finance Group[4] and the Charity Commission[5]. Under each section heading describe what you and your colleagues are actually doing. This will help you identify the policy gaps and process failings that need attention.

A spider diagram representation of your income and expenditure flows can also help you identify particular areas of fraud risk. For example:

- **Income:** grants, legacies, membership direct debits, investments, gift aid, credit cards, cash or cheques, etc. Signing up to a legacy notification service (like Smee and Ford) can also help you get a clearer picture of incoming bequests.

- **Expenditure:** salaries, utilities, VAT, family contributions, expenses, credit cards, depreciation, etc. Grant-giving organisations may also want to include details of awards and recipients.

You should involve the whole organisation in your fraud risk review, so don't forget to gather information and insights from support staff and departments. For example, do you know if the IT team has done penetration tests? Have the findings been acted upon?

Run process test-checks of your own and take the time to observe certain jobs in action. If you receive lots of cash or cheques make sure you understand the post opening procedures and the chain of custody controls that govern them – then go and watch it being done. Do you know how (or if) staff follow-up the mail-out of sponsorship forms and fundraising packs? Would the supporter care team recognise the signs of a fraud and could they deal with it confidently? On your direct debit run, how easy is it to change the destination account and who is allowed to do it? (Charities with direct debit runs of over £1 million a month really need to know the answer to this one).

Take a similar approach to questioning and testing spending-related processes. What controls do you have in place to monitor occasional payments (to new-starters or leavers) and salary changes? Is management information reviewed regularly? Are payroll runs compared so that anomalies can be spotted? Take the time to test-check a number of actual staff expense claims. And if you don't already have regular and frank conversations with your partners and suppliers about fraud risks and fraud reporting, think about starting them.

4 Charity Finance Group (2012). *Charity fraud: a guide for the trustees and managers of charities* (p11).

5 Charity Commission (2012). *Internal financial controls for charities: checklist.*

PEOPLE: YOUR GREATEST ASSET OR WEAKEST LINK?

While people can be your greatest asset, they can also be your weakest link when it comes to fraud prevention. Volunteers, partners and donors are all potential sources of fraud vulnerability, but in some cases it may be a member of your own staff.

Perform proper due diligence in all staff and recruitment matters as well as in your dealings with other third parties. Try to make sure that this careful approach is adopted by your delivery partners as well. When a fraud problem does arise adopt a transparent, open and honest response; it shows the world you are managing the situation properly and tells your staff (and others) that you mean what you say about tackling fraud. Aim to publish good information about your anti-fraud activity. Include the number of fraud events you have had to deal with – don't shy away from reporting cases in which staff members were dismissed, partnerships suspended or vendor contracts cancelled – but also document the significant benefits (including cost savings) of fighting fraud and building resilience.

Staff and volunteer fraud

Charities should take care over the kind of people they employ and recruit them into a workplace culture in which dishonest behaviour is never acceptable.

About half of all frauds against organisations are committed by someone on the inside,[6] and this is no less true for charities. Individual acts of staff dishonesty can range from a lie on a CV or application form to a high value fraud committed by one or more employees (or volunteers) already on the inside.

We all depend on trust among colleagues and partners in our everyday working relationships. No-one likes to imagine that a colleague at the next desk, or the volunteer working in our shop, might be a fraudster. But career fraudsters do quite deliberately seek out positions inside charities precisely so that they can exploit the weak controls and over-reliance on trust they expect to find there. And while most employees would never think of it, the temptations of easy access and lax controls can sometimes prove too much even for a previously honest person.

6 KPMG (2013). *Global profiles of the fraudster: white-collar crime – present and future.* Also see PricewaterhouseCoopers LLP (2014). *2014 Global economic crime survey.*

Because the full cost of an insider fraud – which can include regulatory penalties, disciplinary processes, investigation costs, recruitment of replacement staff, as well as the damage to reputation and staff morale[7] – is so much higher than the headline loss, prevention is much more cost-effective than 'cure'. Effective pre-employment screening is an important part of this.

Basic screening of candidates should include the following.

1. Ask to see original identity documents. (If you're not sure about authenticity use a document verification service.)

2. Check qualifications, either directly through the issuing college/university or via the Higher Education Degree Datacheck service, the UK's official degree verification service. (Since 2009 they have spotted 180 fake universities and 2,700 people submitting incorrect information.)

3. Check work history by taking up references, calling referees and probing employment gaps.

4. Explore opportunities to share your data with other organisations so that a fraudster can't just hop from one charity to another without being recognised. There are established schemes to help you do this.

You should also check on staff periodically during their employment, not just at recruitment. Make it quite clear to new applicants and existing staff that checks will be made.

While prevention is partly about controls like screening, it is also about understanding the individuals you employ and being open about fraud risk so that everyone can recognise the warning signs (red flags) when they see them. Common red flags include sudden and unexplained lifestyle changes, signs that someone is living beyond their visible means,

7 Cifas (2013). *The true cost of insider fraud.*

or a reluctance to take holiday. None of these alone is evidence of fraud – there can be legitimate explanations for all of them – but they do indicate a need to investigate further.

Desperation (personal crises) and disgruntlement (a missed promotion) are both common motives for fraud. Treating staff well – including support for anyone in financial difficulty or who has drug or alcohol problems – can be a really good way to prevent fraud.

Fundraising and donor fraud

Because many charities rely on well-meaning individual fundraisers (frequently volunteers) it can be difficult to know how much money to expect from any given activity. This uncertainty creates opportunities for fraud.

Fundraising fraudsters come in many shapes and sizes. They could be high-value serial offenders who hold one-off events with no intention of donating the proceeds, opportunists who may have started with good intentions, or our old foe the bogus door-to-door collector. Risks typically range from straight-forward theft of collection boxes to the elaborate creation of fraudulent fundraising websites. And the potential harm done is not limited to the revenue lost today; by damaging a charity's reputation and undermining public confidence these frauds can reduce the flow of donations far into the future.

Reducing opportunities for fundraising and donor fraud should be a high priority, so take the time to think hard about your key risks. How might a person or gang go about defrauding your charity? Here are some of the most common scams.

- Stealing clothes from a charity shop or selling them under-value.
- Skimming cash so that not all the money raised is received.
- Low value credit card donations which the fraudster uses to test stolen card details.
- A refund request for a large, bogus donation that was supposedly made in error.
- Misappropriation of legacies intended for the charity.
- Fake door-to-door or street collections and/or events where fraudsters impersonate charity workers.
- Unauthorised or fraudulent use of the charity's logo on third-party websites.
- Creation of fake fundraising websites.

Many of these risks can be tackled with nothing more complicated than well-managed procedures for controlling things like the distribution of branded fundraising merchandise, post-event follow-up and the refund of donations (which should only ever be returned to the original source). Proper systems for credit card validation, identity checks and associated due diligence should all be part of your standard operating procedures.

You should always know exactly what your fundraisers are doing on your behalf. Keep good records so you can scan the activity data for unusual patterns and anomalies. Creating a formal, centralised log of all reports of potential fraud and suspicious behaviour will also help here. If a fundraiser seems extremely reluctant to accept new procedures for the handling of money, you should wonder why. If you receive several reports about collection bags when you are not currently using this fundraising method, you know you have a problem.

Ultimately, if you have concerns about a fundraising event you can always pull out. But if you have a well-documented, well-thought-out, post-event follow-up procedure (especially relating to the money raised and when it will be received) you will be better equipped to spot any fraudsters hiding inside your fundraising team.

UNDERSTANDING AND PREVENTING COMMON FRAUD RISKS

Charities face the same fraud risks as any other sector. All are moving targets. Fraud threats change continuously as fraudsters constantly seek out the greatest benefit for the smallest risk, so our approach to tackling them needs to be just as dynamic. The better protected (fraud resilient) a charity, or any organisation, can make itself, the lower its total cost of fraud.

Fraud can occur at any point in the financial flow, from the moment a donation is made right through to the money being used to deliver services, supplies or grants. Charities are particularly vulnerable to frauds of diversion (such as skimming), extraction (false invoicing) and back-handers (bribes for grants), with risks frequently much greater in countries where business ethics are different.

The latest research suggests that larger charities in England and Wales perform best in the following areas of fraud resilience:

- reporting arrangements;
- zero tolerance;
- designing fraud out of systems and processes;
- inclusion of fraud and corruption in risk registers;
- post-investigation reporting of weaknesses and lessons learnt; and
- consideration of all possible sanctions against the fraudster.[8]

But the same research also shows that there is plenty still to be done in getting anti-fraud staff trained professionally, understanding the true cost of fraud, reviewing the effectiveness of controls and culture, and making more use of analytical techniques to understand and defend against specific threats and risks.

Common fraud risks faced by charities include online fraud, bribery and corruption, and financial fraud. Every charity with some form of online presence – be it a Facebook page, Twitter account or a website – is now at risk of cyber-attack. Bribery and corruption can be a particular threat for charities with extensive international operations. And the traditional reliance on high levels of trust can make the charitable sector especially vulnerable to financial fraud engineered from within.

Online fraud

Criminals are increasingly turning to the internet to steal information and commit fraud. Cybercriminals are often particularly active in the immediate aftermath of a natural disaster or human tragedy, taking advantage of the public's eagerness to help the victims. Most use software and 'malware' (programs designed to facilitate criminal activity) easily found online. Many of them simply play the odds, sending vast quantities of fraudulent communications at a keystroke. An estimated 156m 'phishing' emails (designed to capture private information) are now sent every day; the one-in-ten that makes it through spam filters and into our inboxes is sufficient to trick 80,000 people into disclosing their private information to criminals.[9]

Because online security is mostly about protecting data a few simple precautions can make a big difference. Remind staff and supporters not to open emails from unknown sources. Encourage supporters making online donations or purchases to check that the website is https-secure and be wary of websites or emails containing common spelling or grammatical mistakes. Instruct offsite staff to avoid free public WiFi when connecting to the corporate network.

Staff mobile devices, laptops and PCs should all be protected with anti-virus and anti-spyware tools that are current and kept up-to-date. Any device used to transfer or receive data containing sensitive personal material should be encrypted as well.

Bring your password protocols into line with the latest thinking. Require staff to use passwords that are at least 14 characters with no dictionary-identifiable words, but don't insist they change them regularly. GCHQ (the government security and intelligence centre) now recommends password changes only after a suspected or actual security breach. Requiring staff to change perfectly good passwords routinely is thought to increase the chance of a security breach by making it more likely that the new passwords will be easier to crack.[10]

Don't wait for a cyber-attack to happen before thinking through how you'll react. Create a cyber-fraud response plan as soon as possible. Remember, in the event of an attack you may need to shut down your entire network, so include a detailed action plan for the first 24 hours.

Bribery and corruption

Many charities work in countries where bribery and corruption are serious problems. Ideally corruption should never be acceptable, regardless of how pressing the immediate operational problem might be. The relationship between corruption, poverty and other social ills is well-documented; if a charity allows itself to become involved in corruption it is very probably undermining its own long-term mission. Conversely, if more organisations stand up to bribery it will, in time, become much harder for anyone to demand, make or facilitate a corrupt payment.

8 PKF Littlejohn LLP and the University of Portsmouth (2015). *The resilience of the charity sector in England and Wales 2015: research into how well charities protect themselves.*

9 IT Governance Ltd. *Beware of the (phishing) bait.*

10 GCHQ (2015). *Simplifying your approach: password guidance.*

All charities, but especially those working internationally, need to identify where their main bribery and corruption risks lie, then decide how best to mitigate them. Factors for consideration include the local culture and geography, the charity's own culture and operations, as well as the operational roles played by staff and non-staff participants.

Certain kinds of relationship present the greatest risks. These include your links with partners, suppliers, contractors and consultants who have ready access to substantial amounts of your information or who frequently work closely with your people and systems. Beneficiaries, municipal authorities and anyone involved in recruitment are all sources of bribery and corruption risk, the latter particularly so.

The best approach to tackling corruption is an holistic one. This includes the creation of an organisation-wide anti-corruption culture that deters staff, volunteers and others, improves compliance with the Bribery Act 2010, and closes numerous loopholes. Internal communication and training will play an important part here, along with appropriate policies, procedures and systems supported and reinforced by managerial oversight and review. Make sure you are alert to the signs of bribery and corruption and equipped to respond effectively. Always protect staff who try to stand up to bribery and corruption. Make sure there is always an effective investigation backed by sanctions and mechanisms for redress.

If you are truly committed to preventing bribery and corruption there will be some operational disruptions, so plan for them. But remain resolute; eventually the rewards from your anti-corruption stance will be significant and widely-felt.

Financial fraud

To identify potential fraud in your accounting and financial systems you must do two things: get to know your systems and data (to understand what 'normal' looks like) and perform a fraud risk assessment.

One way to do this is by routine checks such as bank reconciliations (month-end) and stock counts (year-end). Augment these with unannounced spot checks and internal audits to help uncover any existing frauds and deter new ones by keeping everyone on their toes. Log all anomalies and then look for suspicious patterns in the data. If everything looks a bit too perfect be wary of this too – it may be completely made up! Use data analytics to scan datasets (like payroll or direct debit runs) for differences that shouldn't be there, or should be there but aren't. Techniques like these can also shed light on shortcomings in staff training or difficulties using certain systems. Anomalies will need investigating but be careful about jumping to conclusions. What looks like a fraud might really be an error.

Consult other departments, such as logistics or human resources, to make sure you've got the complete picture. Unusual inventory movements or salary payments, for example, might have perfectly legitimate operational explanations.

Ensure your management team monitors your financial controls and applies them consistently. Check that they are fit for purpose everywhere; sometimes an ideal controls scenario won't work 'in the field' and you'll need to take a step back to find a compromise that does.

If you are considering a new activity or project conduct an early fraud risk assessment to help you plan the best risk mitigation controls. And don't forget that your people also need to understand how they fit into the control processes to help them learn from each new incident and grow their anti-fraud skills.

RESPONDING TO FRAUD: WHAT TO DO WHEN THINGS GO WRONG

Fraud happens. It's how we respond that decides how successful we are in resolving matters. So what should you do when things do go wrong?

It is important to act quickly when you discover a fraud. Speed will help you:

- reduce the risk of further losses;
- increase the likelihood of recovering assets;
- protect the organisation's reputation;
- meet the expectations of regulators; and
- keep open the option of a civil injunction as part of your legal response.

In other words, waste as little time as possible.

The Charity Commission expects trustees to report fraud to Action Fraud (the UK's national fraud and cybercrime reporting centre) and then to pursue recovery of the losses where appropriate.[11]

11 Charity Commission (2013). *The Charity Commission strategy for dealing with fraud, financial crime and financial abuse of the charity sector.*

You are also likely to have certain other reporting obligations. The Charity Commission itself will expect to hear from you about any actual or suspected fraud (under its reporting serious incidents regime). If you have fidelity or crime insurance you should notify your insurer immediately because failure to do so might invalidate your policy. (Check your policy conditions carefully. If you are in any doubt speak to your broker.) You might also want to inform your donors, bank and auditors.

Once the fraud has been reported, what then? To respond very quickly you really need already to have a response plan in place, explaining how, when and by whom the fraud will be investigated, reported and resolved. Only the very largest charities have dedicated in-house fraud expertise, so it can also be important to have an agreed procedure for deciding when and how to engage external professional support.

If you are starting from scratch the 'reasonable person' test can serve you well here. What would a reasonable person do in these circumstances? If the loss is relatively small (perhaps, low level skimming by a volunteer in a charity shop) it makes no economic sense to engage a large legal team. But if someone has stolen a whole month's direct debit takings then it's probably time to bring in some serious legal artillery.

A complete legal response to a fraud could have civil and criminal components, but not every option will be available or appropriate in every case.

The criminal route

If you have a real suspicion of fraud you should report it to Action Fraud, though not every case reported will be investigated and prosecuted. Criminal cases that are put before the courts are heard by a jury. For a conviction the case must be proved beyond a reasonable doubt.

As for recovering losses, the Powers of Criminal Courts (Sentencing Act) 2000 (s130(2A) says, *'a court must consider making a compensation order in any case where it's empowered to do so'.* In other words, a successful criminal conviction might be followed by a compensation order, but only if the court deems it appropriate. Compensation is limited to £5,000 in the Magistrates' Court, but there is no limit in the Crown Court.

Even though small frauds are the least likely to be investigated by the police you might still want to report them, if only to make clear that fraud will not be tolerated and that action against fraudsters will always be taken.

The civil route

The primary purpose of the civil legal route is to recover losses. The burden of proof is much lower than in a criminal court; you will need to prove only that it is more likely than not that you were defrauded (or, in other words, the balance of probabilities supports your case).

Civil proceedings are generally more suitable for larger cases where the fraud losses are sufficient to justify the time, effort and expense. That said, you might still want to consider suing the fraudster for smaller amounts if your case is sufficiently clear-cut.

If you do decide to take the civil route, talk to your lawyers (if you have them). If they have a litigation function they should be well-placed to help you. If not, they should be able to refer you to a firm that can. Remember, you need lawyers who are used to dealing with civil cases and who understand the charity sector and its regulatory framework. To maximise your options and your prospects of success they will need to act quickly and know how best to present your case to a judge rather than a jury. If one or more of your employees are among the accused you may need a specialist employment lawyer as well.

Even if you have no budget for litigation, talk to your lawyers just the same. Many firms offer an initial consultation at no cost and will sometimes take the whole case on a pro bono or 'no win, no fee' basis. Helping a charity out of a fix can be great PR for lawyers, so it's always worth a call.

Your lawyer will want to see all the information you have about the defendant and their offence. If it's an inside job you should already have name, address and bank account details (to pay their salary), and possibly some idea of their assets and family situation. A full paper trail for the crime itself will also be needed. A high priority will be to establish the strength of your case and its main weaknesses (if any). A lawyer can also help you begin to quantify the damage done, decide on a course of action and set a realistic budget. On the particular question of harm; if you think the fraud might present an existential threat to your charity get some insolvency advice immediately.

CASE STUDIES

CASE STUDY 1

A trusted charity store volunteer with a gambling habit stole more than £1,000 over a five-month period. Suspicions arose when a new area manager noticed that the store's annual profits had halved. A hidden camera was installed which caught the fraudster failing to register sales through the till and then stealing the cash. He was given a 12-month community order and told to pay £800 in compensation.

CASE STUDY 2

The former head of counter-fraud at a major international aid charity was sentenced to two-and-a-half years in prison after pleading guilty to stealing almost £65,000. Following the Haiti earthquake he had used his own investigation into fellow aid workers as cover for a nine-month scam using false invoices from two fictitious companies. The crime was uncovered following an internal investigation into the fraudster's own professional conduct. During the trial the court heard that he had been addicted to prescription drugs at the time of the fraud.

CASE STUDY 3

A former chief cashier, who had worked for the same major children's charity for 11 years, stole donations worth more than £800,000 by intercepting postal orders and cheques and then changing the name of the payee. He used the money to pay for a luxury house, a villa, cars and various investments. Having pleaded guilty to 19 charges of theft and three of forgery, he was jailed for six years.

CASE STUDY 4

A homeless charity was forced into administration when two members of its finance team, including the head of finance, were arrested on suspicion of widespread fraud. The sum at risk is in the region of £800,000.

Managing internal investigations

Charities are often expected to investigate internal frauds for themselves. Whether or not the suspect is a staff member and/or UK-based, the basic principles of the investigation will be much the same and so will be the main investigatory challenges: problems with slow reporting of suspicious events; controlling the flow of information to those who 'need to know'; waters muddied by keen but untrained people trying to conduct their own preliminary enquiries.

Once an allegation of fraud is made, assess the information for reliability and consequences. How you investigate will depend largely on the resources available to you; can you call on dedicated in-house staff, must you depend on third-party services (which tend to be expensive), or will it be a bit of both?

Before you get started, draw up formal terms of reference for the investigation. This is an important document; it should be realistic and deal in specifics. Set out the objectives, scope and methodology of the investigation. Define the start and finish dates and map-out a plan of work. (Pro-formas can help you with all of this.) The work plan can be much less formal and more flexible. It will help you decide what to do next and will probably change often as the investigation proceeds.

All investigations are a search for evidence that will tend to prove or disprove particular activities or events, or the intentions of the people involved in them. Evidence will come in many different forms: physical, documentary, photographic, electronic (emails or texts), scientific. There will also be 'circumstantial evidence' (information that puts a suspect in the vicinity of the crime at the time it was committed), witness statements, and possibly expert testimony (perhaps from a handwriting expert). The suspects themselves can also be interviewed as part of your evidence-gathering, normally using the non-accusatory, information gathering model known as PEACE. (The US has a similar model of its own.)

Once the investigation is deemed complete you will need to document all of its findings by recording every piece of evidence in a logical and coherent way. The final report should then cover all of this evidence, the statements, and your conclusions. You might also want to add some recommendations, both for action against the offender (people actions) and control changes designed to prevent something similar happening again (process actions). This definitive document should always be written to make sense to someone (usually management) with no first-hand knowledge of the case. You can also use it as the basis of your report to the board. Develop a standard template, with instructions, to make this important job much easier next time round.

Top tips for preventing, detecting and responding to fraud

The first national conference on charity fraud was an important opportunity for trustees, senior managers and their advisors to share experiences, insights and best practice in fighting fraud in the charitable sector. Here is a summary of the top tips that emerged.

GOOD GOVERNANCE AND FRAUD RISK MANAGEMENT

- Prevention is better than cure – and much more cost-effective! Review your processes and procedures and introduce strict accountability to make it hard for anyone to commit fraud in the first place. Never use trust as an excuse for poor risk management.
- Fighting fraud is a job for everyone at every level. Make the in-house case for an ethics programme by focusing on positive behaviours – doing the right thing, setting the right tone, leading by example, supporting staff, building a good reputation – and emphasising the wider benefits.
- Make sure your trustees treat fraud awareness and risk management seriously. Systematically encourage fraud awareness and understanding throughout your organisation.
- Create a framework of strong values and then publicise them in a formal code of ethics. Include examples of day-to-day ethical business dilemmas to help employees and volunteers understand what is at stake and to make good decisions under pressure.
- Understand the risks you face by conducting an annual fraud risk review and then documenting areas of greatest vulnerability in a risk register. Some fraud is inevitable so be clear about how much fraud you are prepared to tolerate (your charity's 'appetite' for fraud risk) and manage the risks accordingly. Have regular and frank conversations with your delivery partners about fraud risks and reporting.

- Conduct process test checks, especially on vulnerable systems. Watch key procedures, such as the opening of post, and do not make assumptions. Do you know how easy is it to change the destination account on your direct debit run? Are your fundraisers following up sponsorship forms that are not returned? Train your supporter care teams properly so that they will recognise fundraising fraud red flags when they see them.

- Adopt a clear and unambiguous whistleblowing (or 'speak up') policy. Give it plenty of support and publicity. Write it with the typical concerns of employees in mind. Who should they talk to? Will something really be done? Are reports truly confidential? How will you prevent retaliation?

PEOPLE: YOUR GREATEST ASSET OR WEAKEST LINK?

- Build a workplace culture in which fraud is never acceptable and everyone knows it. Use your anti-fraud policy to explain this to everyone.
- Replace high levels of trust with high levels of accountability and professionalism. Know what people are doing in your name; keep good records and keep an eye out for oddities and anomalies. Tackle fundraising threats with well-managed controls and good record keeping.
- Remember, where there's cash there's temptation. Find ways to make it easy for staff to do the right thing. Develop standard operating procedures that reduce risk and encourage honesty.
- Get to know your staff and volunteers better. Run pre-employment screening of new recruits as well as in-service checks for established employees – and expect your partners to do the same. Share your knowledge with other organisations so that known fraudsters can't job-hop.
- Offer support to employees in difficulty. Desperation and dissatisfaction are common causes of fraud.

UNDERSTANDING AND PREVENTING COMMON FRAUD RISKS

- Understand your financial systems and data (including payroll and direct debit donations) and get to know what 'normal' looks like so that you can recognise the signs of fraud when you see them.
- When setting up a new office or starting a new project undertake a fraud risk assessment to make sure control systems mitigate actual risks not theoretical or anecdotal ones. Periodic follow-ups will keep things fit for purpose.
- Check that managers really are applying and monitoring your charity's financial and other controls.
- Make sure staff and volunteers who stand up to fraud, bribery and corruption are properly protected.
- If you are truly committed to tackling corruption there will be operational disruptions, so plan for them. Be determined; the eventual rewards will be worth it.
- Educate staff in good online 'hygiene'; be suspicious of websites with mistakes or odd URLs and treat with caution unfamiliar emails containing links and attachments (as well as familiar emails containing unfamiliar links).
- Bring password protocols up to best practice standards. GCHQ now says frequent, compulsory password changes result in less secure passwords.
- Protect staff mobile devices, laptops and PCs with anti-virus and anti-spyware software that is kept up-to-date.
- Encrypt all devices that transfer or receive data containing sensitive and personal material. (There could be implications under ss.7 and 55 of the Data Protection Act 1998.)

RESPONDING TO FRAUD: WHAT TO DO WHEN THINGS GO WRONG

- Act quickly! This will minimise harm done and maximise your legal options.
- Don't panic. Stay calm and follow procedure (wherever you can).
- Know in advance who needs to be informed (both within the charity and outside it).
- Ideally, have a fraud response plan ready so that everyone knows what to do and when. It should include the critical, 'golden hour' activities that must be done the moment you discover a fraud.
- Take steps to preserve evidence (including electronic communications). Your own investigation will need this later and so will any court action (criminal or civil).
- If you want to recover your losses be prepared to use more than one legal route.
- Seek professional legal advice where appropriate, especially if you think you might take action in the civil courts.
- Remember, the Charity Commission is there to help you. It is important to keep it informed and to follow its regime for reporting serious incidents.


THANK YOU FOR YOUR SUPPORT

Useful resources

Charity fraud: a guide for the trustees and managers of charities

Charity Finance Group
Guidance on how to prevent and detect fraud, as well as information on what to do when fraud is uncovered and where to report it.

Cyber streetwise

HM Government
Practical advice on how to protect your organisation against online crime, as well as links to other useful resources.

Fraud: prevention is better than cure

Crowe Clark Whitehill
Guidance on how to prevent, detect and respond to fraud using assurance frameworks, the three lines of defence model and an understanding of common risks.

Get safe online

Get Safe Online
Practical advice on how to protect yourself and your organisation against fraud, viruses and other common online threats.

Giving safely: a guide to making sure your donations really count

Fraud Advisory Panel
Advice for the giving public on how to donate safely to charities on the doorstep, on the street and online.

Guideline fraud response plan

Charities Internal Audit Network
A sample fraud response plan that you can tailor to meet the specific circumstances of your charity.

Internal financial controls for charities (CC8)

Charity Commission
How to manage your charity's financial activity and use internal financial controls to reduce the risk of losses from fraud and error. Includes a self-assessment checklist to help trustees and their advisers evaluate performance against legal requirements and establish good practice.

Password guidance: simplifying your approach

GCHQ
Practical advice on using a simplified approach to password-setting policies in any organisation.

Say no toolkit

Institute of Business Ethics
A free app and website providing immediate practical guidance to help employees make tricky decisions in difficult situations. The tool is especially useful for any small organisation lacking a formal anti-fraud policy but wanting to provide general support to staff on handling gifts, hospitality, conflicts of interest, and bribery and corruption.

SUPPORTED BY

Crowe Clark Whitehill

Crowe Clark Whitehill has been listed as the lead provider of audit and related services to charities for seven consecutive years. Its services, offered worldwide, include fraud prevention, detection and response.
croweclarkwhitehill.co.uk

ACKNOWLEDGEMENTS

Our sincere thanks to all the speakers who contributed to this first national charity fraud conference, 'Tackling fraud in the charity sector: making your money count', held in London on 30 October 2015: Louise Bailey (Macmillan Cancer Support), Mark Baynham (Plan International), Robert Browell (Macmillan Cancer Support), Dave Carter (British Council), Peter Clarke (Charity Commission), Steven Fennell (Exchange Chambers), Philippa Foster Back CBE (Institute of Business Ethics), Pesh Framjee (Crowe Clark Whitehill), Andy Fyfe (City of London Police), Jim Gee (University of Portsmouth and PKF Littlejohn LLP), Mike Haley (Cifas), Dr Stephen Hill (Fraud Advisory Panel), Laura Hough (Save the Children International), Mindy Jhittay (Bates Wells Braithwaite), Martin Lewis (independent consultant), Caroline Lovelace (WWF-UK), Oliver May (Oxfam GB) and Jo Pearce (Help for Heroes).

Our thanks also go to those students and staff of the University of Portsmouth and the University of the West of England who acted as rapporteurs on the day: Samantha Bourton, Madeline Cosgrove, Dr Axel Palmer and Martha Pritchard.

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