

Keeping fraudsters at bay

It might be easy to think that internal fraud is a private sector crime which charities need not worry about. Unfortunately, that thinking would be wrong. David Adams finds that while charities are just as vulnerable to dishonest employees as businesses, there are a number of precautions they can take to keep from getting stung

Ah, the nightmare that is fraud. Hugely expensive and disruptive at the time, it can also mean massive legal fees further down the line, and can do terrible damage to the reputations of individual charities and of the sector as a whole.

And while there is still an instinctive feeling in many parts of the charity sector that this is not something that happens to not-for-profit organisations, there are plenty of unfortunate incidents that prove it certainly does.

The Helston Downland Trust, a grant-making body in Cornwall, was the victim of a spectacular fraud perpetrated between 1999 and 2003, during which period the clerk to the trustees, Nicholas Walker, stole more than £300,000. An investigation by the Charity Commission found that Walker, under little direct supervision, had changed bank mandates so that they required only his signature, rather than three, and that trustees had been persuaded to sign cheques on which the name of the payee had not yet been entered.

Walker was later jailed for five years. In late 2003 Joseph Mulcahy, founder of the Dream Foundation, (a charity that offered holidays and gifts to terminally ill children) along with his wife Maureen Lewis and David Foley, a former police officer, was sentenced to five years for stealing £100,000 from the organisation. Foley and Lewis received lesser custodial sentences.

There's no reason anyone should be very surprised. The cost of employee fraud to business continues to rise, according to recent research from accountancy firm BDO Stoy Hayward, up by 30 per cent between 2004 and 2005 to about £1bn, while the value of employee fraud has increased by more than 80 per cent since 2004, and by 200 per cent since 2003.

The charity sector may be very different in important ways, but the largest charities now operate like large corporations, while smaller charities tend to have more informal processes in place, thus arguably creating opportunities for fraudsters. There's no doubt that many of the same issues apply.

Protecting the organisation

The most important step in protecting the organisation against fraud is to recognise that it is more likely to be perpetrated by staff than by anyone else, says Andrew Durant, partner in charge of fraud investigations at BDO Stoy Hayward. "Employees are by far the biggest risk, either working by themselves, or in collusion with someone else on the inside or on the outside," he says.

Nor is this simply a problem with untrustworthy temps or

volunteers. Evidence suggests that the risks actually increase with the seniority of staff. So the battle against fraud needs to start at the recruitment process, and checks on employees' backgrounds and references need to be more rigorous for senior appointments. Durant suggests looking as far back into an applicant's career as possible, rather than relying on references that cover only the last few years.

"We have come across people who've had a track record but then kept their nose clean for a few years," he says. Durant also suggests charities check educational qualifications, asking to see original certificates, to see if individuals are prepared to lie to get the job.

There are IT systems and services that can help make this screening process faster and more efficient, such as the URU identity verification system developed by GB Group, which automatically matches individuals across a series of data sets all accessed securely through BT's secure web services platform.

"It allows you to have a risk-based approach," says Karyn Bright, head of marketing for the data authentication division at GB Group. "You don't want to throw everyone out if there's a small problem, but it's good to have a system that shows where you need to ask for further information." The system can also be used to verify passport numbers, which are almost impossible to forge.

"Using an automated system means you're no longer relying on staff being able to spot a fraudulent document or information," says Bright. "It's also saving the time they might otherwise spend making phonecalls, sending faxes or letters checking things out, so you're cutting soft operating costs too."

Sixty-five per cent of the fraudsters questioned in the BDO Stoy Hayward research said their main motive was greed, way ahead of the next most important motives, connected to gambling and debt, and accounting for 11 and 10 per cent respectively. So, evidence of inexplicable wealth can be an

indicator of something untoward. "Look out for people living beyond their means," says Durant. "One of the first things I do when I start an investigation is actually to walk around the car park, looking for the most expensive cars. That may sound silly, but if someone's stealing money people don't tend to put it in the bank. They spend it on cars, holidays, on the latest electronic goods – then show them off."

You should also watch out for staff starting to behave in ways that seem out of character or unusual. One classic sign is the employee who never takes a holiday or works very long hours. "Fraud is a full-time job," explains Durant. "People have to do their day to day work and then do the fraud and cover their tracks. That may mean they're unwilling to leave the office, especially if someone else is going to be doing their job while they're away so might see something they don't want them to see."

BDO Stoy Hayward also commissioned a survey of 1,500 UK employees, carried out by the pollster organisation YouGov, which showed that nine out of ten would report dishonest colleagues, but that many were put off doing so by fears of the consequences. This may be in part because of media publicity of the negative consequences corporate and government whistleblowers have suffered in recent years, suggests Durant. "People may be frightened," he says. "Whistleblowers always seem to be the ones who lose their jobs or are ostracised.

There needs to be a culture where they are seen as the saviours of the organisation, rather than as 'grasses'."

There is also a need to try and engender a good ethical culture, which again, may sound odd in connection with a charity, but the YouGov survey threw up some alarming attitudes; for example, more than one in ten of those questioned said they thought it was "sometimes acceptable" for managers to award contracts to companies owned by their friends, or secretly owned by a relative, or for them to accept gifts in

return for contracts being awarded. "You can't assume people will always know what's right and what's wrong," says Durant. These issues should be covered in an employee code of conduct.

As far as more formal protective measures are concerned, charities would be well advised to examine how and where money comes into the organisation. It may be necessary to implement and enforce strict procedures for opening mail from donors to guard against cheque-based fraud. Charities also need to be aware of the possible consequences of a lack of supervision of regional or international offices. An example of the problems that can arise in connection with the latter was in the news earlier this year, when Oxfam was forced to admit that "weak management and monitoring systems" were to blame in part for the loss of £11,800 that was supposed to have been used to help post-Tsunami recovery and reconstruction efforts in Indonesia, but was appropriated en route.

"The further you get from the centre the less visibility there is over what happens to the money, and people are more likely to think that if they tried something they'd get away with it," warns Durant. "If charities have operations away from headquarters elsewhere in the country, it's key that operations people get out to visit those sites and find out what's happening."

There are other signs that may indicate fraudulent activity, such as new staff leaving the organisation unexpectedly, or unrecognised transactions on the charity's bank statements, or those of service providers or donors. It may also be worth keeping an eye on an individual working for a service provider who insists on only ever dealing with a particular member of staff.

Finally, if a charity does suspect fraud it must proceed every slowly and carefully, starting in almost every situation by seeking legal advice – an incorrect accusation could lead to an employment tribunal, or breaches of the Human Rights Act or the Data Protection Act – and more awful publicity.

Some tell-tale signs of fraud

1. Staff/volunteer's lifestyle suddenly more extravagant, featuring expensive cars, holidays, clothes or gadgets
2. Changes in behaviour – fraud is a stressful business, so are the gambling and addiction problems sometimes associated with it
3. Staff working long hours regularly for no particular reason, failure to take holidays, reluctance to delegate work to others – "fraud is a full-time job".
4. New staff resign and leave the organisation unexpectedly and suddenly, without leaving clear information about where they are going
5. Unexplained rises in operating costs
6. Mysterious anomalies on the organisation's bank statements, or those of suppliers
7. Excessive expenses claims
8. Unusually close relationships with particular suppliers or other business partners; suppliers who insist on speaking to one member of staff only