CHARITY COMMISSION
FOR ENGLAND AND WALES

Protecting charities' funds

Detecting fraud against charities

Introduction

The harm that fraud can cause to charities' good work, their beneficiaries and reputation, as well as to public trust and confidence in the sector, can be immense. Increasingly, the public and donors expect charities to play their part in this fight and to demonstrate what action has been taken to mitigate the risk of fraud. A better understanding of the frauds that charities are facing will allow timely dissemination of learning and best practice, in order to build the resilience of all charities to the growing threat of fraud.

Although recent years have seen a number of new guides and publications to assist charities, no analysis of frauds committed against charities has ever been published. This paper helps to address this gap and is the first in a series of publications, guidance and advice from the Charity Commission ('the commission') and partner organisations.

Background to this data

The commission's 'serious incident reporting regime' (RSI Regime) has been in operation since 2007 and is an important compliance and monitoring tool, both for individual charities and for the sector as a whole. It allows the commission to maintain oversight of trends and problems affecting the wider sector, and to put charities back on a secure footing where problems have occurred. There is a dedicated reporting line (**RSI@charitycommission.gsi.gov.uk**).

During financial year 2015/16 over 2,200 serious incidents were reported to the commission by charities, of which 178 were classified as fraud. For the first time, the commission has analysed a sample of RSI fraud submissions to identify sector wide learning points. It sampled fraud related RSIs from a broad range of charities - small, local organisations such as school PTAs, to large well-known charities with thousands of staff and multi- million pound budgets.

Key findings

Review of the commission's sample of fraud RSIs noted:

- that over a third of the frauds sampled were 'internal', meaning frauds originating within the charity (for example perpetrated by trustees, staff or volunteers)
- highest single reported loss to fraud was over £1 million
- common identifiable trends in many of these fraud cases include weak governance and poor financial controls, often coupled with excessive trust placed in key individuals within the charity
- several cases related to fraud carried out by charities' overseas partners, where the legal and regulatory context can often be difficult to manage; this suggests potential problems with excessive reliance on trust as a key control - this highlights the need for enhanced due diligence and oversight for those charities working with international partners
- cyber-enabled frauds, often where social engineering has played a part, are relatively common; these include 'Mandate' fraud, where charities are deceived into diverting legitimate payments to fraudsters' bank accounts; or 'chief executive' fraud, where fraudsters, often using publicly available information, impersonate senior officers of the charity and trick charity staff into making payments made to the fraudsters' bank account

What charities can do to address these issues:

- review and implement the commission's guidance – **Internal financial controls for charities (CC8)** and the **Compliance toolkit chapter 2: Due diligence, monitoring and verifying the end use of charitable funds**
- robust and consistent application of existing controls
- develop a culture of professional scepticism and appropriate challenge
- raise staff awareness of mandate fraud and the social engineering tactics of fraudsters
- become familiar with the government's **'Cyber Essentials'** toolkit; and consult guidance and good practice available on the new dedicated Counter-fraud website for charities **www.charitiesagainstfraud.org.uk.**

Case Study 1: Internal fraud

A charity reported that the trustee/treasurer had misappropriated approximately £15,000 of charity funds, with a series of unauthorised payments being made to family members. A £5,000 investment of the charity was cashed in without authority and the treasurers' personal expenses were found to have been met out of charity funds.

Learning point: clearer, agreed segregation of duties and closer oversight of financial transactions (by a trustee other than the treasurer) would have identified this fraud earlier.

Case study 2: 'Chief executive' fraud

Following receipt of a fraudulent e-mail purporting to be from the charity's chief executive, the finance director made a payment of £15,000 to an unknown bank account. No checks were made to ensure the message was bona fide.

Learning point: check all such payment requests are from a genuine source; challenge payments made to unknown bank accounts; consistently apply existing controls and procedures, even when requests are made from senior officers.

Case study 3: 'Social engineering' fraud

A charity was defrauded of £10,600 (in 3 transactions) by a telephone/online scam. The charity treasurer received a telephone call from an individual claiming to be from a major telecoms company, offering a £400 inconvenience fee for the telephone problems supposedly suffered by the charity in the previous year, and to 'clean' the charity computer for free. When the treasurer agreed, despite not having previously had problems with the phone, the fraudster took control of the computer and subsequently made payments to the fraudsters' bank account.

Learning point: always be suspicious of seemingly 'too good to be true' offers of assistance. Never give access to charity laptops to unknown/unverified individuals or organisations.