Charity fraud – latest research and lessons for trustees

Charity Fraud Awareness Week 2023

Charity fraud – latest research and lessons for trustees

Speakers:
Kristina Kopic, Head of Charity and Voluntary Sector, ICAEW.

Louisa Burton, Researcher, University of Portsmouth.

Laura Hough, Director of Trust & Ethics, ICAEW.

Matthew Field, Head of Fraud Advisory Panel.

Charity Fraud Report 2023

Key Findings & Trends

- 67% agree cost of living has increased fraud risk.
- 36% have experienced more instances of fraud since 2022.
- 56% experienced non-financial costs (morale, reputation), with 65% more than one.
    - 2022: 36% said no impact other than financial.
    - 2023: 14% said no impact other than financial.
        - Morale & reputation the top two.
- On average, each charity experienced ***three*** different types of fraud.

Charity Fraud Report 2023

Future Risks

- 48% cited lack of internal resource as barrier to fraud prevention.

- Barriers to fraud prevention:
  - (1) Overreliance on trust (57%) (2) lack of resources (48%) (3) lack of awareness (35%).

- 50% felt fraud prevention investment had stayed the same.
  - 64% expected the risk to increase in the next 12 months.
    - Investment to prevent the costs of fraud?

Charity Fraud Report 2023

Steps and Actions

- 75% took more than one type of action.
- 2022: 34% recouped some of their losses, in 2023 this rose to 44%.
- 2023 report contains *Top tips for preventing fraud (page 20 - 22).*
  - *Insider fraud*
  - *Payment diversion*
  - *Cyber*
  - *Expenses*
  - *Donation*
  - *Grant*
  - *Procurement*
- ***Fraud Response Plan (page 22)*** *"Have a plan so that you are prepared".*

Case Study 1: Legacy Fraud

- Assets including cash and property valued at around £1.5-2M were left to a charity in a donors last will and testament.
- Significant income for a small charity and would have funded two important programmes.
- The donor was known to the charity but had not been in contact or donated for several years, the charity were not notified of this legacy.
- The donor's solicitor (registered and regulated in the UK) diverted funds for their own personal use.

Case Study 1: Legacy Fraud

Impact

- Working hours lost to the police investigation (still pending after 2+ years) legal action and admin time in recovering the assets.
- By the time the assets were recovered they had diminished significantly in value.
- Significant impact on charitable objectives and activities (due to lost time and money).

Charity Fraud Report & CFAW 2023

- Control Measures

- Keep good records so that you can scan activity data for unusual patterns and anomalies, including contact with regular donors and supporters.
- Audit trails that cannot be deleted or over-written for electronic and paper records.
- Segregation of duties and responsibilities according to job roles and system access rights.
- Carry out regular closure reviews for all legacy files to make sure that all income is properly accounted for.
- Regular progress reviews carried out on outstanding legacies.

- Response measures

- ***Nature of relationship with donor, how often did they previously donate?*** Were the communications regular then they stopped? How do you engage with those close supporters?
- Contact friends or close relatives to gather information about the deceased's affairs (if practicable).
- Report the incident to your relevant national law enforcement agency and regulators.
- Always ask for and analyse third-party valuations of estate assets and liabilities and seek independent validation of assets and liabilities

Case Study 2: Grant Fraud

- A potential beneficiary applied to an organisation for help with their energy bills.
- They applied multiple times using names of friends and family in the area.
- Staff at the charity became suspicious (due to distinctive voice) and reported it to police
- Ultimately, they confronted the individual themselves.

Case Study 2: Grant Fraud

Impact

- Lost time and resource that could have helped genuine applications.
- Genuine beneficiaries harmed (their details had been falsely used).
- Reputational damage - faith lost perhaps from the genuine beneficiaries who were affected.
- Dilemma – what do we do when we are suspicious of claims for help – we want to help people.
- Disappointment in the police response – morale of employees.

Charity Fraud Report & CFAW 2023

- Control measures

- Risk assessment to identify high-risk applications.
- Regular monitoring and auditing procedures.
- Ensure that your grant management system is fit for purpose, captures information accurately and is ***easily accessible for checks and cross-references*** through the grant management process.
- Have robust due diligence procedures with strict eligibility criteria, conduct appropriate level of background checks on applicants, and verify the accuracy of information provided in grant applications.

- Response measures

- Importance of having a response plan to take action that counters and contains immediately.
- Good counter fraud culture to recognise fraud to mitigate the risk and minimise harm.
- System that reviews activity and claims to identify any patterns such as type of claim, ***location***, identity.
- Detailed analysis for common links across systems, phone numbers? Addresses? Voice recognition?
- ***Good preparation and planning*** will ensure effective and timely decision making.

Case Study 3: Cyber

- Finance officer received an email from the chief officer advising them of a change to their bank details.
- Email appeared genuine, appeared to come from a genuine email address and contained personal name details of both the recipient and the sender.
- Finance officer amended the payroll details and paid the monthly salary to the fraudster.

Case Study 3: Cyber Fraud

Impact

- Financial.
- Cybersecurity and internal systems.
- GDPR
- Reputation.
- Trust and morale.

Charity Fraud Report & CFAW 2023

- Control Measures

- Training and awareness of staff.
- The latest trends and scams being deployed by fraudsters (i.e. what a phishing email might look like).
- Ensure your policies reflect the current working environment in relation to the digitised and technology focused processes your charity uses.
- Separate systems? (Multi factor authentication). [LH: Documented process for changing financial details including independent verification.]
- Counter fraud culture with open ***communication and reporting confirm and reconfirm details***.

- Response measures

- ***Review your IT security solutions and practice. Secure? Fit for purpose?***
- Perform a cyber-fraud risk assessment, where cyber fraud risks are identified, risk rated and assigned to a responsible individual for managing.
- Know what to do in the event of accidentally clicking on a link from a phishing email and have ***timely reporting processes (inform the bank, HR, payroll).***
- Ensure you are prepared to act quickly if a cyber-related incident occurs (i.e. have a cyber response plan).

Emerging risks

- Emerging areas must always be considered but we have identified that current threats remain prevalent (insider, supplier, APP).
- Threats will always evolve: Voice cloning, false document production, ID theft.
- AI & Chat GPT as a defence? There are tools out there designed to recognise false documents, voice recognition software and serve as a guide to use.
- Be proactive in your prevention approach.
- “What is your fraud response **PLAN?”.**

Charity Fraud Awareness Week 2023

The role of AI?

How can a charity use AI to prevent fraud?

- Implement machine learning algorithms to analyse transaction patterns, detect anomalies, potential fraudulent activity, enhance ID verification processes.

- Regular updating and training to the AI model is “crucial to adapt to evolving fraud techniques”

- **How can I use AI to do that?**

- (1) Data collection (2) Feature engineering (3) model selection (4) train the model (5) Real time monitoring (6) alerts and reporting (7) Continuous improvement (8) integration with ID verification (9) COLLABORATION with experts.