Briefing note: COVID-19 fraud and the VCS

It has been widely reported that fraudsters are currently seeking to exploit the situation with COVID-19.

Action Fraud reported an increase in coronavirus related fraud by 400% in March. Annually, fraud is currently estimated to cost the charity sector in the region of £1.9 billion every year already.

With large volumes of people self-isolating and working from home, cyber-crime has undoubtedly increased. Cyber security breaches can include:

- Phishing emails, where others impersonate an organisation online;
- Viruses or other malware, such as ransomware (a form of software preventing effective control of data stored on a device until a ransom is paid).

The complexity of cyber-crimes is ever evolving and it can be increasingly difficult to detect. In order to be best protected against all types of fraud, organisations need to regularly review their own potential exposure and take the necessary steps to guard against the threat of fraud as well as have a plan in place to ensure an effective response if fraud is detected.

Kingsley Napley[1] has identified some critical questions, that they suggest organisations should ask themselves to help prevent fraud:

Risk assessment

1. Consider which of the organisations activities leave it most vulnerable to fraud. For example, does only one individual have sole charge and responsibility for financial processing and reporting or does the organisation have a large number of volunteers that are more difficult monitor?
2. Look at the level of fraud awareness within the organisation. Is the organisation alert to the potential new fraud risks, such as phishing, cyber-hacking of financial accounts and interception of email communications to third parties containing sensitive financial information?
3. Does the organisation have an appropriate anti-fraud policy? The purpose of this is to provide a definition of fraud and define authority levels, responsibilities for action, and reporting lines in the event of suspected, attempted or actual fraud.

Fraud detection

1. Spot the warning signs - for example red flags might be irregular invoicing, a sudden change in an employee's behaviour or missing documents or records.
2. Implement staff training and make it known that everyone associated with the organisation has a responsibility for being vigilant and keeping an eye out for any signs of fraud.
3. Publish a procedure dealing with how to report suspected fraud confidentially.
4. Ensure thorough checks and controls are in place (these could be computerised and/or manual processes).

Response

1. Assemble a core team of people to work together to investigate and combat the fraud. Depending on the size of the charity, consider identifying representatives from Human Resources, IT, Finance and the Management Team.
2. Take steps to ensure that the fraudster is not aware that you have identified the potential fraud. It is very important that any evidence is preserved.

[1] https://www.kingsleynapley.co.uk/insights/blogs/litigation-for-charities-blog/how-to-guard-against-and-respond-to-fraud-in-the-charity-sector

3. Conduct a thorough investigation with a detailed record (but be alert to the fact that any documents created may have to be disclosed in subsequent legal proceedings).
4. Consider the legal options. You may want to terminate the employee's employment, involve the police in bringing a criminal prosecution or bring a civil claim to try to recover funds.

The Fraud Advisory Panel have set up a COVID-19 fraud watch group which is a cross-sector and cross-industry coalition of trusted partners (including the Cabinet Office and City of London Police) who meet weekly to share information on emerging fraud threats and trends affecting business. It aims to act as a conduit to warn the public, private and third sectors about COVID-19 fraud risks and the preventative actions that can be taken.

Current COVID-19 fraud risks include:

- Password spraying campaigns
- Misuse of corporate vehicles for fraud (phoenix companies)
- Government impersonation on social media (esp. DWP)
- Phishing emails (e.g. UK Business Advice Bureau and travel companies)
- COVID-19 domain names (e.g. PPE mask-related)
- Payment diversion / mandate fraud
- Malware
- Courier fraud

Anticipated and/or emerging issues include:

- Increases in fraud and insolvencies as a result of desperation, financial difficulty and economic uncertainty.
- Government funding applications on behalf of legitimate businesses by fraudsters.
- India's symptom checker app 'JIO' has been compromised to harvest personal data. Fraudsters are expected to target similar apps in the UK, as well as apps more generally.
- Fraudulent streaming sites, with the initial offer often coming via WhatsApp.
- Advanced Persistent Threat groups targeting healthcare, pharmaceutical companies, academia, medical research organisations, and local government to collect bulk personal information, IP and intelligence on national policy or research.
- Fraudsters looking for supply chain, website and network (including VPN) weaknesses.

Tips for prevention:

- Suspicious emails should be sent to the NCSC at **report@phishing.gov.uk.**
- Businesses should carry out risk assessments for staff working remotely, and conduct due diligence on customers and suppliers.
- Use BACS instead of faster payments if possible.
- Consider reducing thresholds for payments requiring enhanced authorisation.
- Watch out for app-based phishing emails and spoofed apps, particularly related to the new NHS tracker.
- Fraud Advisory Panel, Charity Commission and the Small Charities Coalition, along with other sector partners, are issuing a free webinar on COVID-19 and charity fraud on 12 May, available **here.**

Tackling Mandate Fraud

1. **Verify:** If you receive a request to move money into a new bank account, contact the supplier directly using established contact details, to verify and corroborate the payment request.
2. **Internal processes:** Establish robust internal processes for handling changes to payment details. For example, only designated employees should be able to make changes to payment arrangements.

3. **Sensitive information:** Invoices, payment mandates, and other documents containing sensitive financial information should be stored securely and only be accessible to those staff that need them to perform their duties. Sensitive documents should be shredded before they are disposed of.
4. **If you have made a payment**: Inform your bank as soon as possible, they can help you prevent any further losses. Monitor your bank statements regularly for any unusual activity.