Not For Profit

Preventing fraud in Not For Profit organizations

Fraud is a serious problem that can potentially affect everyone, from individuals to large companies and associations.

csae | scda™†

Canadian Society of Association Executives
Société canadienne des directeurs d'association

While fraud can originate from outside, it can also be perpetrated by individuals within an organization. For Not For Profit (NFP) groups that devote their time and resources to advancing worthy causes, fraud — both external and internal — can affect your organization's ability to fulfill its financial mandate and can generate a negative image in the public sphere. This can result in damage to your reputation and loss of credibility, leading to longer term funding shortfalls and associated challenges.

There are a number of ways to minimize the potential for fraud and its effects on your organization. Understanding different types of fraudulent activity and educating yourself and your associates about how it occurs and how to identify it is a good place to start. From there, you can incorporate procedures using a system of checks and balances to help prevent fraudulent activity from occurring in the first place.

RBC Royal Bank®

RBC®

The importance of internal controls

Forensic accountants say when fraudulent incidents occur, they're typically not discovered internally — they're found through outside tips or by accident.

The Association of Certified Fraud Examiners' findings indicate fraud can occur for up to 18 months before being detected.

A recent PriceWaterhouseCoopers survey indicates that insufficient internal controls is one of the top three reasons for committing fraud. When an employee or volunteer realizes there are loopholes to exploit, in some cases it's an opportunity too tempting to resist. Fraud can erode up to roughly 6% of an organization's revenues. It's essential that organizations know the warning signs and establish clearly defined fraud prevention precautions and procedures — especially applicable to anyone who handles cash.

Fraud prevention measures

Establish internal controls

Separate cash handling duties

- Wherever possible, ensure no single individual is responsible for handling cash, issuing cheques or reconciling bank statements.
- Having two signing authorities for issuing cheques is considered a best practice.
- If changes are made to signing authorities, ensure these are documented in bank authorization forms.

Implement rigorous cash handling procedures

- Make bank deposits promptly by using night deposit services offering 24/7 flexibility.
- Issue individual payments for all expenses so they can be matched to a specific invoice.
- Keep chequebooks, cash and returned bank statements with cancelled cheques under lock and key.
- Consider credit cards or electronic payments to replace cheques when making payments.
- Reconcile all payments with a vendor invoice or other paper document.

Conduct background checks

- Do basic background checks on all associates — paid or unpaid:
  - Contact personal and professional references.
  - Consider conducting a check for known criminal activity.
- Require bonding of associates who handle funds.

Set up accounting policies

- If you have auditors, have them set an auditing policy to aid in detection of fraudulent accounting or bookkeeping.

Fraud prevention measures cont'd

Establish internal controls

How to prevent cheque fraud from affecting you

- Refuse to accept any cheque that you cannot prove is legitimate.
- Check the date and signature and look for any alterations such as changes to the dollar amount.
- Keep tight controls on your own cheques.
- Reconcile bank statements frequently — daily is the best practice.

Signs a cheque is "bad"

- Issuing bank's name, address, etc. are missing.
- The word "Void" appears on the cheque.
- The cheque is not signed.
- MICR numbers at bottom of the cheque:
  - Are missing
  - Don't match the cheque's serial number
- Stains or discolouration indicate possible tampering.
- The cheque number is missing or did not change.
- There are typeface inconsistencies (name style is different from address or amount, etc.).

Identity theft — protecting your brand from fraud

- Always be on the lookout for identity or brand "pirates" who may assume your association's identity or that of other legitimate charities for the purpose of soliciting funds.
- Encourage associates, donors and the public alike to report any suspicious communications/solicitations.

Safeguarding your information technology (IT) infrastructure

Your information systems contain the lifeblood of your organization: donor/member information, financial data and more. Therefore, it's critical you implement a security policy specifically for IT governing the use of all data, servers and networks, as well as hardware, such as laptops and external drives. This is especially important in instances where associates work offsite and/or after hours. Regular system monitoring, including email monitoring, is both a defence and a deterrent.

Steps for avoiding IT security breaches

- Secure all computers — especially laptops.
- Establish information security protocol for CD/DVD burners and external drives.
- Never respond to emails soliciting passwords (i.e. "phishing" or "spoofing").

If you suspect fraud, immediately follow these steps

- Disconnect the source of the intrusion.
- Isolate corrupted systems.
- Shut down relevant servers or hubs to prevent further access to the system.
- Contact the carrier or ISP to attempt to trace the attack.
- For major breaches, consider contacting the police.

Avoiding mail fraud

Incoming mail

- If you suspect mail theft, report it to your local postal station and the police.
- Retrieve mail promptly.
- Ensure mailbox is locked (if applicable).
- Replace wall-mounted mailbox with a mail slot.
- Appoint a responsible individual for all mail duties.
- Ensure the mail repository is visible at all times.

Outgoing mail

- Never place outgoing mail in your mailbox.
- Avoid using street mailboxes.
- Send high value cheques via registered mail or wire transfer.

Fraud prevention measures cont'd

Establish internal controls

Sound business practices

- Implement a formal code of conduct.
- Develop an appropriate expense policy.
- Close account(s) if credit card or bank statement theft is suspected.
- Don't use Social Insurance Numbers (SINs) as employee numbers.
- Provide fraud prevention training for staff.
- Shred paperwork containing sensitive data.
- Secure all sensitive data (personal identifiers, account numbers, etc.).
- Implement password protected computer access, changing passwords frequently.
- Change your personal identification number (PIN) regularly.
- Issue unique passwords for each individual employee.
- Restrict access to data based on relevance to the employee's position.
- Conduct random audits on business accounts.
- Never accept cheques payable to any party other than your organization.
- Never cash cheques for friends by depositing the cheque and issuing cash.

The tips and advice presented here are by no means exhaustive; there's a great deal of information available to help your organization establish fraud detection and prevention protocol.

Partnerships worth protecting

RBC Royal Bank® is a proud sponsor of the Canadian Society of Association Executives (CSAE), with a relationship spanning 15 years. We're equally proud of our tradition of community involvement, special event funding and association with a variety of philanthropic initiatives. As such, we understand the specific needs of not for profit associations. Our dedicated team of national not for profit relationship managers offers cost-effective solutions, including investments and cash management tools, designed to maximize your resources.

To learn more about CSAE and its wealth of resources available, please visit **www.csae.com**.

To find out more about fraud detection and prevention, as well as a range of financial solutions for your not for profit organization, please visit **www.rbc.com**.

VPS52825

07460 (09/2009)