Preventing fraud in not-for-profit organizations

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

For a not-for-profit group like yours, fraud — both external and internal — can be particularly devastating. Not only can it affect your organization's ability to fulfil its financial mandate, but it can also generate a negative image of the organization in the public sphere. This could lead to a damaged reputation, loss of credibility, longer-term funding shortfalls and other associated challenges.

There are a number of ways to minimize the potential for fraud and its negative effects on your organization. Understanding the different types of fraudulent activities and educating yourself and your associates about how fraud 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.

The importance of internal controls

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

> "From January 2014 to December 2016, it is estimated that Canadians lost over $290 million to fraudsters."[1]

A recent study completed by the Association of Certified Fraud Examiners found the presence of anti-fraud controls correlated with both lower fraud losses and quicker detection. In a comparison of organizations that had certain anti-fraud controls in place with organizations that lacked these controls, it was found that where certain controls were present, fraud losses were 12% to 56% lower and detected more quickly.[2] 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 5% of an organization's revenues in a given year.[3] 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 — How to establish internal controls

Separate your payment-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 they 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 detecting fraudulent accounting or bookkeeping.

Prevent cheque scams

- Refuse to accept any cheque 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.

Protect your brand from identity theft

- 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.

Safeguard your IT infrastructure

Your information systems contain the lifeblood of your organization: donor/member information, financial data and more. Therefore, it's critical you implement an IT security policy specifically for 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 or after hours. Regular system monitoring, including email monitoring, is both a defense and a deterrent.

To avoid IT security breaches:

- Secure all computers — especially laptops
- Establish an 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:

- 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

Tips to avoid mail fraud

Incoming mail

- If you suspect mail theft, report it to your local postal station and the police.
- Retrieve mail promptly.
- Ensure your mailbox is locked (if applicable).
- Replace your wall-mounted mailbox with a mail slot.
- Appoint a responsible individual to handle all your 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 by registered mail or wire transfer.

Signs a cheque is “bad”

- Issuing bank’s name, address, etc. are missing.
- “Void” appears on the cheque.
- Cheque is not signed.
- MICR numbers at the bottom of the cheque are missing or don’t match the cheque’s serial number.
- Stains or discolouration indicate possible tampering.
- Cheque number is missing or did not change.
- Typeface inconsistencies (name style is different from address or amount style, etc.).

About business email compromise (BEC)

BEC scams often begin with a fraudster successfully compromising a business executive, a high-level employee related to finance or any publicly listed email account. This is usually done using key logger malware or phishing methods, where the fraudster creates a domain that’s similar to the domain of the company they’re targeting (or a spoofed email) to trick the target into providing account details.

Monitoring the compromised email account, the fraudster will try to determine who initiates wires and who requests them. These perpetrators often perform a fair amount of research, looking for a company that has had a change in leadership, has publicly announced a merger/acquisition or is undertaking a significant construction development or renovation project. Then they use the event as an opportunity to execute the scam.

Some common BEC scams

- **Fake invoice scam** — Fraudsters often use this tactic to target companies with foreign suppliers. The attacker pretends to be a supplier requesting payments by fund transfers to an account owned by the fraudster.
- **CEO fraud** — The attacker poses as the company CEO or an executive and sends an email to employees in the finance department requesting them to transfer money to the fraudster’s account.
- **Account compromise** — An executive’s or employee’s email account is hacked and used to request invoice payments to vendors listed in their email contacts. Payments are then sent to fraudulent bank accounts.
- **Attorney impersonation** — The attacker pretends to be a lawyer or someone from the law firm supposedly in charge of crucial and confidential matters. Normally, such fictitious requests are done by email or phone, and at the end of the business day.
- **Data theft** — Employees in HR or bookkeeping are targeted to obtain personally identifiable information (PII) or tax statements of employees and executives. Such data can be used for future attacks.

Because these scams do not have any malicious links or attachments, they can evade traditional solutions. Employee training and awareness can help enterprises spot this type of scam.

Spotting brand phishing and spoofing

This is a scam where a fraudster sends an authentic-looking email, appearing to come from a legitimate company, to acquire personal and financial information. The email address is altered to very closely resemble a legitimate email address.

Examples:

- Legitimate: Companyname.com
  Altered to: Companyname.us (“.com” changed to “.us”)
- Legitimate: Companyname.com
  Altered to: Companynarne.com (“m” changed to “r” and “n”)

Establish authentication protocols

The purpose of this procedure is to verify a sender’s request for payment or changes to standing instructions.

A simple call to a telephone number on file can verify whether the requested changes are legitimate and large payments have been authorized. This will go a long way to avoid unauthorized disbursements and suspicious or fraudulent activity.

Consider using authentication protocols when:

- A fax, letter or phone call seems out of character or not in line with previous transactions
- Instructions have been sent by email or a text message (even if the sender's address or cellphone number appears to be valid)
- A sense of urgency is expressed
- The amount requested is above the established internal limit

Sound business practices

- Implement a formal code of conduct.
- Develop an appropriate expense policy.
- Close the account(s) if you suspect credit card or bank statement theft occurred.
- Social Insurance Numbers (SINs) should not be used 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 a unique password to each employee.
- Restrict access to data based on its relevance to the employee's position.
- Conduct random audits on business accounts.
- Never accept cheques payable to any party other than your organization.

We are proud of our tradition at RBC Royal Bank® of community involvement, special event funding and associating 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.

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.

To find out more about fraud detection and prevention, as well as a range of financial solutions for your public sector entity, please visit www.rbcroyalbank.com/not-for-profit.

RBC®

[1] "Fraud Facts 2017 – Recognize, Reject, Report Fraud," Competition Bureau, Government of Canada, February 28, 2017, https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04201.html

[2] "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse," Association of Certified Fraud Examiners Inc., 2019, https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

[3] Ibid