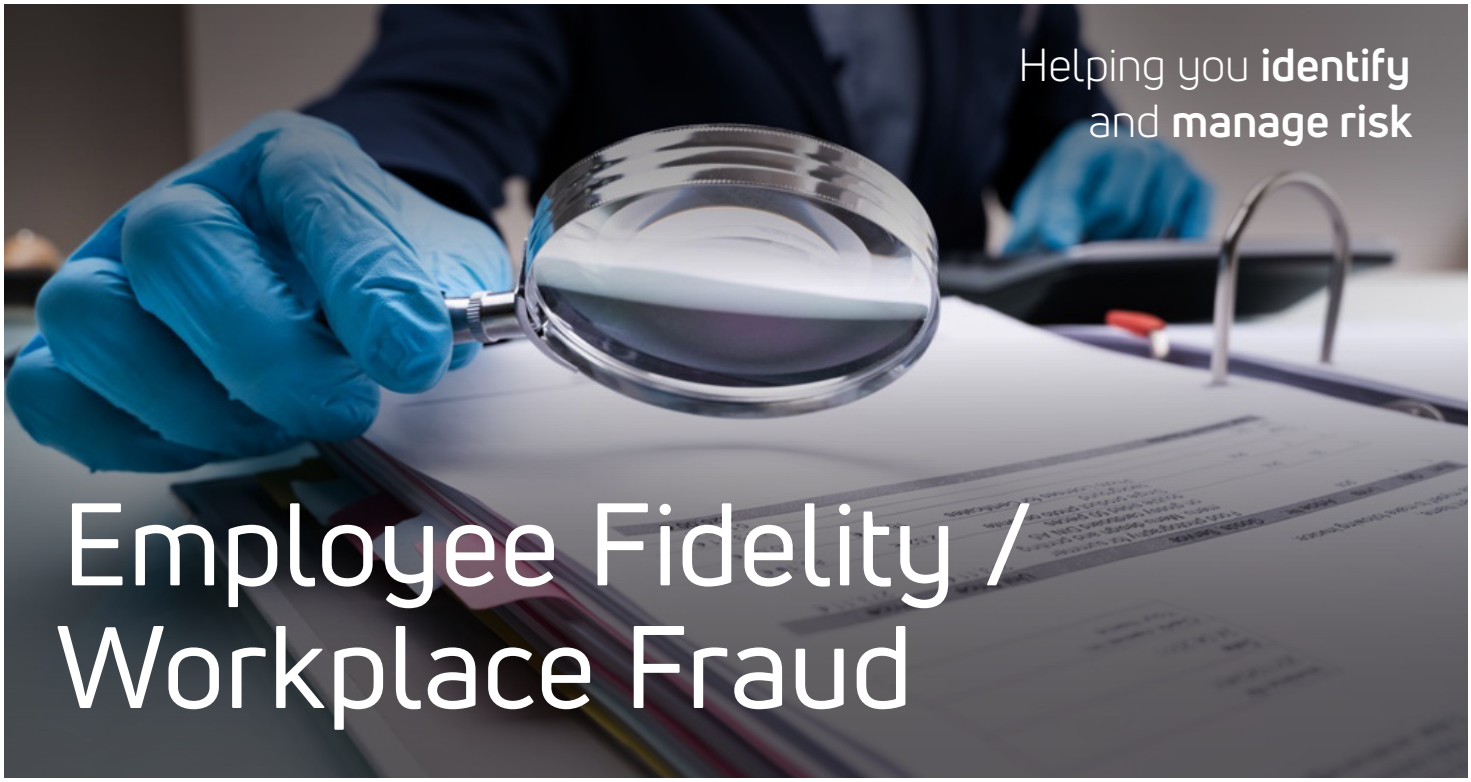
ecclesiastical

Bulletin



Employee Fidelity / Workplace Fraud

Disappearing petty cash... false billing... bogus cheques... altered expense claims... credit card fraud... financial misrepresentation...

Theft occurs in all kinds of organizations including small, not-for-profit agencies, retirement homes, schools, and faith communities. Sadly, the culprits are often 'insiders' – managers, employees and volunteers who were once valued and trusted members of the community.

Employee fraud ranges from simple theft – taking donations from a collection box in a place of worship or stealing cash and other valuables in a care home – to cheque forgery, bogus invoices, and elaborate accounting schemes. In some cases, employees have diverted small sums on a regular basis. Over a period of years –even decades– this may add up to very large amounts of money.

According to the Association of Certified Fraud Examiners (ACFE), the typical fraud case in Canada results in an average loss of some $90,000 with statistics showing billing schemes to be the most common, present in more than a third of fraud cases.[1]

Employee Fidelity/Workplace Fraud

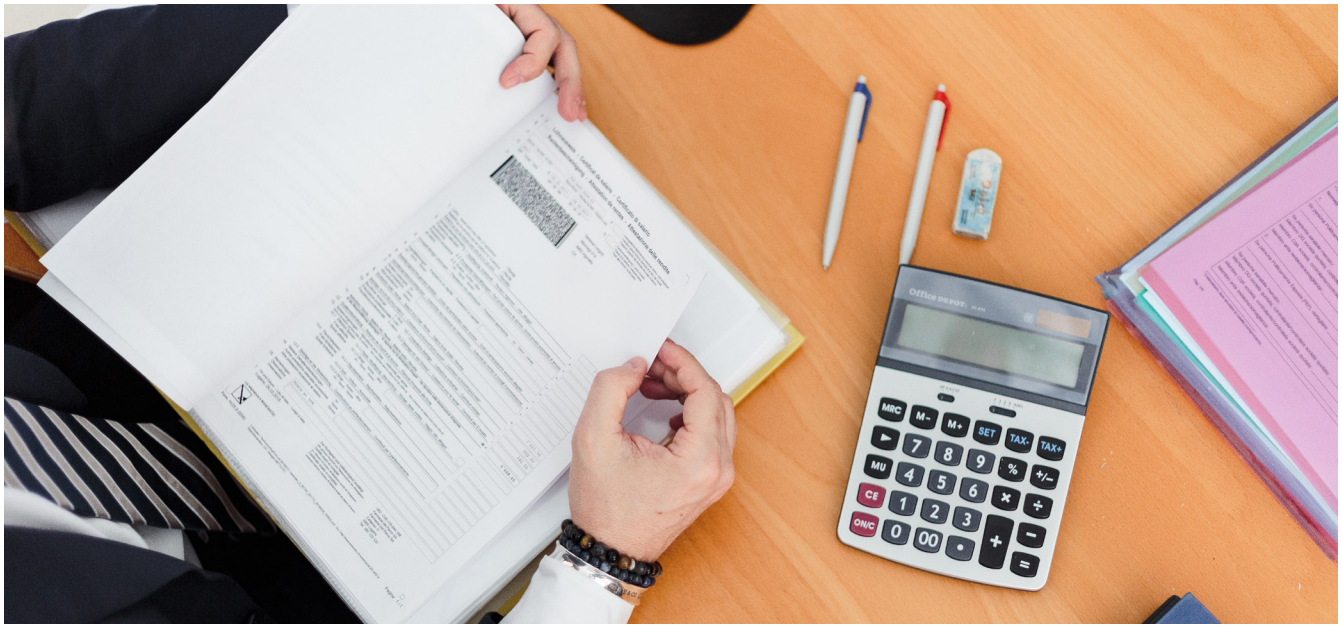
Occupational fraud can occur in all kinds of organizations including small, not-for-profit agencies, retirement homes, schools, and faith communities. Many non-profit organizations are often more susceptible to fraud because they may lack many of the controls necessary to prevent a loss and will be impacted the most financially.

The culprits are often 'insiders' – executives, managers, employees and volunteers who were once valued and trusted members of the community.

There are three main types of occupational fraud: corruption, asset misappropriation and financial statement fraud.

Signs of fraud include being unable to reconcile monthly financial statements; changes in individual behaviours: lifestyle change (living beyond their means); working longer hours than required; and not taking time off work for fear of fraudulent actions being detected in their absence. Fraud can be hidden by creating or altering existing hardcopy documents or electronic documents.

The first step in dealing with employee dishonesty and fraud is to recognize that the risk exists in virtually every organization. The next step is to identify and assess vulnerable areas where fraud might occur - for example, payroll, cash donations, banking, bookkeeping, ordering of supplies, etc. This fraud risk assessment exercise should not be limited to your organization's leadership. By including employees and volunteers, even in an informal way, you send a clear and powerful message about your organization's standards and the benchmarks you have set for workplace behaviour.



Best Practices

The following are among the best practices that can help your organization prevent, deter, and detect workplace fraud.

1. Background and Credit Checks

Include background checks as part of your hiring practices- criminal checks, employment history verification, education verification and reference checks. The same checks should be performed when bringing volunteers on board. Include credit checks for individuals who will have access to financial information, handling of vendors or suppliers, cash, or other funds.

2. Code of Conduct

Develop a Code of Conduct that includes policies, processes and controls to prevent fraudulent behavior. Make sure that everyone reads it and signs a form acknowledging that they have done so and that they agree to the policies and procedures outlined.

3. Anti-Fraud Policy

An anti-fraud policy is an essential tool that can help to defend your organization against fraud. An anti-fraud policy can formalize your approach to fraud prevention, establish the controls required and outline what action will be taken against those committing fraud. It is a good idea to include Human Resources in developing this policy. The policy shows employees and the public that the organization has an anti-fraud culture, and that fraud will not be tolerated. The policy should be reviewed with all new employees and volunteers upon hiring and it should be refreshed and signed off annually. Keep the signed copies in the individual's HR file.

4. Audits

Conduct internal and external audits regularly. Inform everyone that audits are routinely undertaken, and that information is actively sought regarding fraudulent behaviour. In addition, perform surprise audits to combat and detect fraud.

5. Management Review

To further support your organization's anti-fraud culture regular management reviews should be performed on internal controls, processes, accounts, transactions, and certification of financial statements.

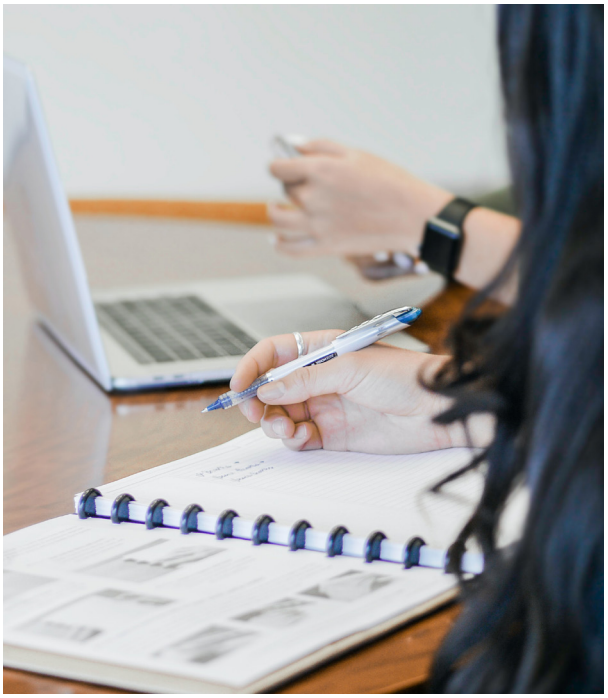
6. Account Reconciliation

Perform monthly account reconciliations using the bank reconciliation and the monthly bank statement, along with cheque images. To reduce possible fraudulent activity, the account reconciliation should be performed by an individual who does not handle the accounting/finances, vendors and purchasing.

Part of the account reconciliation includes verifying the names of vendors. Vendors should be on the approved list and match the name on the cheque. Research and investigate any unknown vendors and reason for expense to verify it is a legitimate expense or potentially fraudulent.

7. Training

Fraud awareness training should be provided for all managers/executives, employees, and volunteers.



8. Whistle-blower hotline

Develop a way for people within the organization or outside of the organization such as a customer, vendor, or contractor to 'anonymously' report violations or suspicions of fraudulent behaviour.

9. The Two-Person Rule

Establish a dual control system for handling funds. A policy that requires two people in unrelated positions and unrelated personally to handle money will greatly reduce both the temptation and the opportunity to steal.

10. Separation of Duties

Have more than one individual share in tasks to maintain internal controls.

11. Access

Keep the number of employees who have access to financial matters as small as possible. When you minimize access, you minimize risk.

12. Vendors and Suppliers

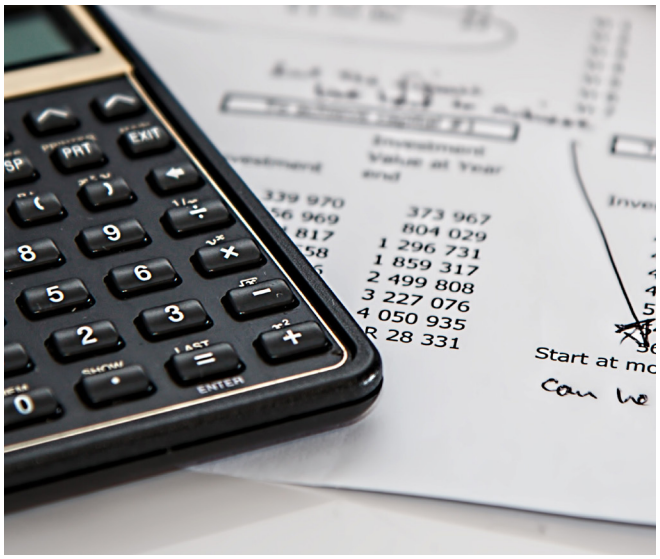
To avoid phony invoices and other billing schemes, make sure that vendors and suppliers have been vetted and approved. Consider sharing your Anti-Fraud Policy with these third parties to show you have controls in place to detect and prevent fraud.

13. Formal Approval Process

Set dollar limits for employees and volunteers who order products and services. Beyond these limits, additional signatures would be required.

14. Financial Records

All records should be safely stored from both physical loss and digital loss. For example: records stored in areas where water damage can occur such as the basement should be raised off the floor by at least 6 inches. Another way to prevent physical loss is to store records digitally and back them up offsite using the cloud, or offsite servers. IT professionals should be consulted with to ensure they are stored properly and are protected from cyber-attacks.



Some further considerations include:

15. Cyber-Attacks

Financial losses can also be a result from cyber-attacks known as social engineering were cyber criminals trick people by sending out fake emails, texts, and voice messages that can appear to be from a friend, co-worker, or a trusted source in hopes of obtaining passwords and financial information. Regular training should be provided to staff and volunteers that have access to the organization's computers, passwords, and financial information to ensure they are on alert for possible social engineering attacks. Visit our website at https://ecclesiastical.ca to access our Risk Control document on Cyber Risk Management.

16. Donations

If your community accepts cash donations, make sure that they are deposited on the same day and not left overnight. Use the two-person rule to have funds counted and deposited. The two-person rule should also be implemented for donations that come in by mail. If funds must stay on your premises, keep them in a safe or a locked office. If possible, ask regular donors to use electronic funds transfer to make donations.

17. Job rotation

Where possible rotate individuals on duties and tasks to prevent and detect fraud. It is encouraged that both employees and volunteers take mandatory vacation (ideally 2 weeks in a row) to assist in detecting potential fraud in their absence.

By implementing these best practices and, if possible, by establishing a finance committee to oversee all financial matters, your organization will go a long way towards mitigating the risks of workplace fraud and protecting your reputation. By safeguarding your donations, you will also be safeguarding the trust of your donors.

In the event you encounter suspicions or allegations of fraud, be sure to involve Human Resources and legal counsel in the investigation to determine the best way to act which may include disciplinary actions and local law enforcement for pursing criminal charges. Using professionals to determine the best course of action can save an organization from potential legal implications such as employment-related claims.

If you need legal or Human Resources assistance, contact your broker, an Ecclesiastical Risk Control Specialist or visit our website at **https://ecclesiastical.ca** for details on how to access these free services through our third-party service provider LegalConnex and HRAssist.

Financial losses can also result from cyber-attacks. For further information on cyber risk management visit our website at **https://ecclesiastical.ca**

Reference

Association of Certified Fraud Examiners (ACFE's) 2020 Report to the Nations on Occupational Fraud and Abuse. https://www.acfe.com/report-to-the-nations/2020/

https://www.canadianunderwriter.ca/features/opportunity-for-fraud/

http://lrzconsulting.com/reviewing-bank-reconciliations-to-prevent-and-detect-fraud/

ABOUT ECCLESIASTICAL INSURANCE

Ecclesiastical Insurance Office plc is a specialist commercial insurance company. We are deeply committed to protecting the needs of organizations that enrich the lives of others; to preserving Canada's distinct communities, cultures and history; and to supporting initiatives that help improve the lives of people in need.

ecclesiastical | BENEFACT GROUP

Proudly part of the Benefact Group - specialist financial services companies built to make a difference.

ecclesiastical.ca | @EIOCanada