



EMPLOYEE FRAUD: IS YOUR ORGANIZATION AT RISK?

A GUIDE FOR FRAUD PREVENTION, DETECTION AND RESPONSE

EMPLOYEE FRAUD

IS YOUR ORGANIZATION AT RISK?

If you operate a business, it's likely that at one time or another, you will be faced with fraud.

Fraud is a highly problematic issue impacting companies of all sizes, in all industries and sectors. While external threats do represent a portion of fraud risk, all too often the threat comes from within, posed by the very employees trusted to help run an organization.

According to the Association of Certified Fraud Examiners (ACFE), a typical organization loses an estimated five percent of its annual revenue to fraudulent activities. However, the losses associated with fraud typically extend far beyond the misappropriated cash/other company assets, such as reputational damage, lost productivity, loss of future opportunities/donations/support, cost of investigations, cost of prosecution, and the cost to establish safeguards to ensure it doesn't happen again.

In addition, fraud can take a devastating toll on employee morale, especially in smaller companies where relationships tend to be more tight-knit. The shock of knowing that a trusted employee or colleague was capable of such deceit can perpetuate further mistrust and interfere with everyone's ability to focus on their job function. Additionally, being associated with a company undergoing a fraud investigation is often embarrassing for employees who might feel they'll be stigmatized if they choose to pursue a career elsewhere.

The good news? There are a number of steps companies can take to minimize the opportunity for employees to commit fraud, simply by taking a proactive approach. To help you protect your organization, this guide provides an overview of common employee fraud activities, examines typical red flags, offers advice on implementing processes to lessen risk in your organization, and explains what steps to take should fraud occur in your company.



► Fraud losses tend to increase the longer a perpetrator has worked for an organization.

COMMON TYPES OF EMPLOYEE FRAUD

Employee fraud is defined by the ACFE as 'the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets,' and is often the byproduct of opportunity. According to many fraud experts, most organizations are operating within the 10-10-80 rule, meaning 10 percent of employees will never steal no matter what, 10 percent will steal at any opportunity, and 80 percent will go either way depending on how they rationalize their behaviour when an opportunity to commit fraud presents itself. How effectively a company minimizes its risk of fraud is directly linked to its influence over this 80 percent group to limit the opportunities available to commit fraud and reasons for potential ways to rationalize fraudulent behaviour.

Prevalence of the types of employee frauds may vary from one industry to another. Generally speaking, the most common types of employee fraud include:

- theft of cash
- under the table payments, bribes or kickbacks
- creating and paying fictitious suppliers
- theft of incoming cheques
- cheque tampering (forged signatures, altered dates/amounts)
- payment to fictitious employees
- creating inflated or phony expense vouchers
- theft of inventory/supplies

- falsifying receivables and stealing the payments
- altering accounting records to hide the theft of funds
- expense account abuse

The best way for companies to limit opportunity is through the establishment of a clear code of conduct, implementing checks and balances and encouraging all employees to speak up if they suspect fraud.

FRAUD RED FLAGS?

Unfortunately, no matter how many safeguards and processes are implemented, your organization will always have some level of susceptibility to fraud. Despite the common misconception that fraud is primarily a problem in large corporations, smaller organizations are among the most vulnerable, as they lack the resources to administer and adhere to strict processes.

In many cases, fraud starts out small and grows over time in frequency and severity as the perpetrator gains confidence. Educating employees to spot red flags can help detect fraud in its early stages as well as deter potential fraudsters from following through on a plan.

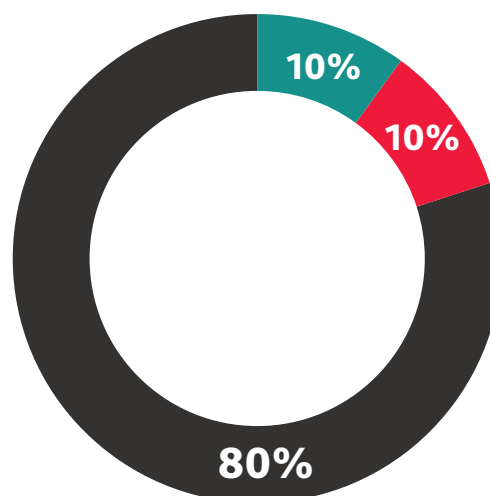
According to the ACFE, 92 percent of all internal fraud cases had at least one of the following red flags displayed by the perpetrator. Though not all employees who display these characteristics are committing or planning to commit fraud, remaining vigilant can help employees at all levels better detect fraud in its infancy.

- Living beyond their means

Do the expensive cars and extravagant vacations seem out of place?

- Financial difficulties

Is an employee facing personal financial problems?



- Employees who will never steal
- Employees who will steal at any opportunity
- Employees who will go either way, depending on their rationale

- ▶ Unusually close relationships with vendor/customer

Does an employee appear overly protective of a relationship? Do vendors insist on dealing with one particular individual?

- ▶ Control issues—unwillingness to share duties

Is an employee reluctant to take vacation or be away from the office?

- ▶ Wheeler-dealer attitude

Is an employee (usually upper management) displaying unscrupulous or dishonest behaviour?

- ▶ Divorce/family/addiction problems

Personal problems are often a catalyst for fraudsters, though many who commit fraud for these reasons claim they intend to correct their actions down the road (i.e. repay the money) once their personal crisis has been resolved.

- ▶ Defensive behaviour

Does an employee overreact when questioned?

PROFILING A FRAUDSTER

Though, given the right opportunity, virtually anyone is capable of committing fraud, statistics show that perpetrators are typically males (64.6% of incidences in Canada in 2016 according to ACFE) between the ages of 31 and 50. Employees who hold management positions and/or a finance function within the company are more likely to commit fraud.

Not only are males responsible for a larger number of frauds than females, they generally cause greater losses.

(source: 2016 Report to the Nations)

Meanwhile, older individuals tend to steal much more than their younger

counterparts. The correlation between higher levels of seniority and higher quantum of loss is due to the higher trust bestowed upon those individuals given their longer tenure and positions of authority.

STOP FRAUD BEFORE IT STARTS

Though you can never fully defend your organization from fraud largely due to the human element, there are a number of ways to mitigate risk. To begin, all organizations should undergo an internal fraud risk assessment that involves a thorough company review in order to identify departments, locations, or processes that present significant fraud/misconduct opportunities. Rate the risks based on likelihood and impact, and develop internal controls and processes to help remediate these risks. Processes don't need to be costly or complicated and can include:

1. THOROUGH EMPLOYEE SCREENINGS

Hiring the right employees is one of the best ways to prevent fraud from occurring. Perform background checks on all potential employees. This should go beyond checking references to involve screening an applicant's criminal history, verifying their education and previous employment history, performing a credit check if they are to be involved in the company's finances, and checking for past drivers' license violations if applicable to their job function.

2. CLEAR EXPECTATIONS AND TRAINING

Even with proper checks and balances during the recruitment phase, potential fraudsters are still likely to slip through the cracks. Limit the opportunity to successfully commit fraud by training all employees on your company's policies and procedures. Establish a clear code of conduct that states specific expectations and consequences and have all employees review and sign

off annually. It's also vital for management to set the tone at the top by stringently adhering to all processes and procedures.

3. DIVIDE EMPLOYEE RESPONSIBILITIES

Segregate duties evenly amongst your staff members to ensure that you are never giving any one employee the opportunity to exploit any organizational and/or accounting weaknesses. For example, regardless of seniority, never make one employee responsible for purchase approvals/invoice approvals, payments or bookkeeping.

4. PHYSICAL CONTROLS

Control physical access to high-risk areas in your organization. This can be achieved with key or access card entry points in various locations. Limit employee access to areas that are essential to their job function and install cameras in sensitive areas to act as a further deterrent. Maintain an access log and require all vendors and visitors to sign in during and after business hours.

5. VENDOR SELECTION AND REVIEW PROCESS

Limit the likelihood of working with inappropriate vendors by getting to know who you're doing business with. Identify your organization's needs and hold a request for tenders. Carefully evaluate all submissions, check references, and conduct regular performance reviews once you've made a final decision.

6. COMMISSION PERIODIC AUDITS/ SPOT CHECKS

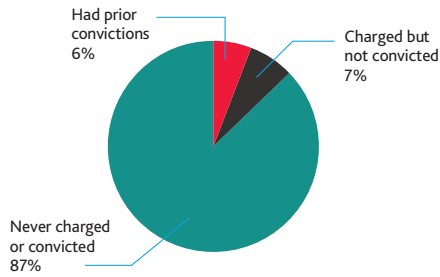
Having a professional, impartial eye reviewing your company's books can help deter potential fraudsters from following through on a plan. It also provides a regular check and balance that can pinpoint suspicious activity in its early stages and stop it before too much damage can be done.



COMMON FRAUD MISCONCEPTIONS

- ▶ Fraud usually happens in certain types of organizations
- ▶ Fraud doesn't happen in well-run organizations
- ▶ Fraud is usually committed by senior employees
- ▶ Fraud schemes are usually complicated
- ▶ Fraud is committed by criminals
- ▶ Fraud is committed by disgruntled employees
- ▶ Large organizations are most vulnerable to fraud
- ▶ Fraud is difficult to detect

Criminal history of fraud perpetrators



Aside from recovering losses, punishing perpetrators of employee fraud is one of the most important steps an organization can take, as it sends a clear message that fraud will not be tolerated.



7. IMPLEMENT AN ANONYMOUS REPORTING SYSTEM

The ACFE's Global Study indicates tips are by far the most common method of discovering fraud.

Establish an anonymous ethical (whistleblower) hotline that makes it easy for all employees/vendors to report suspected incidences of fraud. Ensure your employees understand that all reports will be treated confidentially without reprisal. Consider rewarding employees who speak up.

FRAUD HAS BEEN DETECTED —NOW WHAT?

Despite undergoing an internal fraud risk assessment and implementing the right processes and controls within your organization, you've spotted potential fraud red flags. How should you proceed? This is likely a highly emotional time and you might be tempted to confront the suspected fraudster immediately. However, it's important to proceed rationally, as actions taken at the outset can significantly impact the outcome of an investigation. The moment you suspect fraud, start documenting dates and gathering as much evidence as possible, but try to remain discreet. If a fraudster suspects they've been found out, they will likely attempt to cover their tracks by destroying evidence.

According to the ACFE's 2016 Global Fraud Study, fraud perpetrators with a university degree caused a median loss of US\$200,000, while those with a postgraduate degree caused a median loss of US\$300,000. These figures are significantly higher than the losses caused by less educated fraudsters.

YOUR NEXT STEPS SHOULD INCLUDE:

1. CALL YOUR LAWYER

When you suspect fraud is occurring, retain legal counsel immediately. An experienced fraud lawyer can advise you on the necessary steps to be taken based on your circumstances, including how to proceed with a fraud investigation, strategies to recover losses, and coordination with authorities, as may be required.

2. RETAIN INVESTIGATIVE AND FORENSIC ACCOUNTING EXPERTS

Forensic accountants, while working with lawyers, are experienced at tracing the money (funds/assets), conducting interviews, fact finding, conducting related financial analysis and presenting findings in writing or in the form of oral testimony.

3. SECURE ASSETS

Restrict the employee's access to relevant systems/programs/data. Take control of their office, computer(s) and cell phones, and any other electronic devices provided by the company.

4. DEAL WITH THE EMPLOYEE(S)

Be as discreet as possible when confronting potential fraudsters. Consider suspending the employee with pay pending the outcome of the fraud investigation. During the investigation period, provide the employee(s) with an opportunity to address the issues at hand and clear their name.

5. ADDRESS EMPLOYEE CONCERNS

Don't forget, this is also an emotional time for your remaining employees. Create open lines of communication and keep employees up to date on all relevant information they should know.

DON'T WAIT UNTIL IT'S TOO LATE

When it comes to employee fraud, the most frequently exploited organizational weakness is typically a lack of internal controls. Whether your organization is large or small, establishing and

adhering to stringent anti-fraud policies can help lessen your risk. Investing time and money now can save you much more time, money and undue stress down the road—get started by testing the effectiveness of your organization's fraud prevention policies with the checklist below.

IS YOUR ORGANIZATION FRAUD-PROOF?

- Does your organization properly screen employees and vendors before bringing them into your organization?
- Do employees understand what constitutes fraud?
- Do employees understand they can anonymously report fraudulent activities without fear of reprisal?
- Is management setting the right example?
- Are employee duties properly segregated?
- Does your company undergo random audits?
- Do you uphold a zero-tolerance policy when fraudsters are discovered?

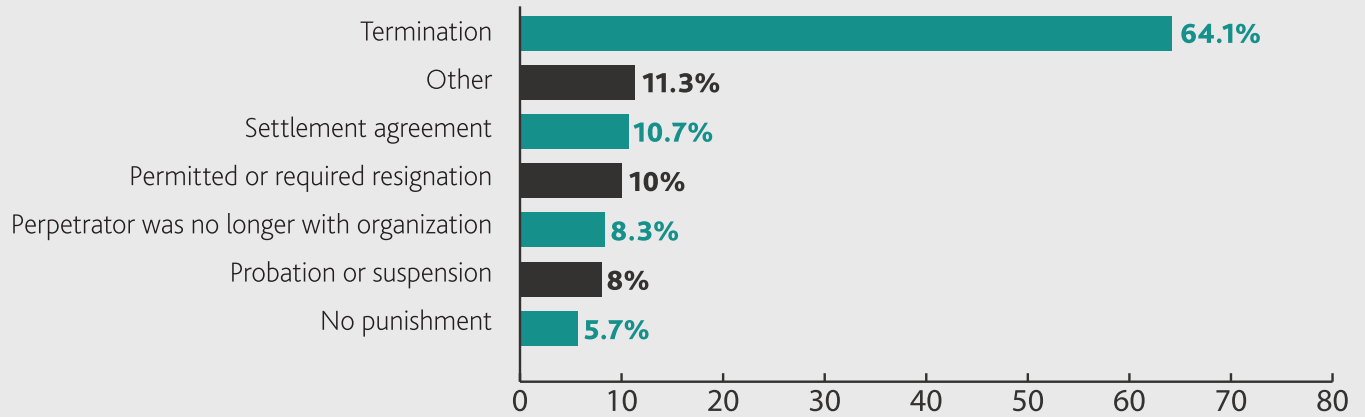
EMPLOYEE FRAUD FACTS AND FIGURES

- ▶ A typical organization loses an estimated 5 percent of its annual revenues to fraud
- ▶ Median loss is extremely costly at an estimated \$145,000 per organization
- ▶ Many fraud incidences occur for 18 months on average before detection
- ▶ Over 58 percent of cases have no recovery of losses
- ▶ Fraud is committed by employees at every level of an organization
- ▶ The more individuals involved in an occupational fraud scheme, the higher the losses tend to be



According to the ACFE's 2016 Global Fraud Study, how did victimized organizations typically take action against fraudsters?

ACTION TAKEN AGAINST PERPETRATOR





HOW IS FRAUD DISCOVERED?

▶ Tips	42.2%
▶ Management review	16.0%
▶ Internal audit	4.1%
▶ By accident	6.8%
▶ Account reconciliation	6.6%
▶ Document examination	4.2%
▶ External audit	3.0%

OUR SERVICES

BDO understands the devastating impact fraud can have on an organization and are able to provide the scrutiny and guidance companies need when it matters most. Whether it's implementing the processes to deter fraud from happening or assisting with the investigation once fraud has been committed, our team of certified fraud examiners, anti-money laundering specialists, financial forensic professionals, and investigative and forensic accountants can provide the help you need.

FRAUD MITIGATION

To help limit the opportunity to commit fraud, we can guide your organization through the risk assessment procedure, conduct fraud/risk assessments, provide training, establish governance structures, and assist with the development of appropriate individual roles, responsibilities and reporting requirements.

POST-FRAUD SERVICES

BDO's Investigative and Forensic Accounting team offers strategic guidance to help clients in all industries navigate fraud occurrences. If applicable, we issue reports suitable for use in court, provide oral and written testimony, and assist in settlement negotiations.

BDO'S INVESTIGATIVE AND FORENSIC ACCOUNTING SERVICES INCLUDE:

- ▶ Internal Corporate Fraud Investigations
- ▶ Forensic Accounting and White Collar Crime Investigations
- ▶ Investigative/Reputational Due Diligence
- ▶ Bribery/Corruption and Money Laundering Investigations
- ▶ Funds and Asset Tracing
- ▶ Litigation Support and Expert Testimony
- ▶ Fraud Prevention and Compliance Programs
- ▶ Anti-Money Laundering and Anti-Corruption Compliance

Whether it's training board members and senior management or safeguarding against cybersecurity attacks, BDO professionals have the experience needed to pinpoint your organization's weaknesses to help you stay protected from fraud. Contact us today to get started.

ABOUT BDO

BDO is a leading provider of professional services to clients of all sizes in virtually all business sectors. Our team delivers a comprehensive range of assurance, accounting, tax, and advisory services, complemented by a deep industry knowledge gained from nearly 100 years working within local communities. As part of the international BDO network, we're able to provide seamless and consistent cross-border services to clients with global needs.



FOR MORE INFORMATION:

CHETAN SEHGAL

Partner, Forensics & Litigation Support
Toronto ON
416-775-7812
csehg@bdo.ca

ROSANNE WALTERS

Partner, Forensics & Litigation Support
Vancouver BC
604-688-5412
rwalters@bdo.ca

GREG HOCKING

Partner, Forensics & Litigation Support
Toronto ON
416-775-7800
ghocking@bdo.ca

ANNE-MARIE BÉLANGER

Partner, Forensics & Litigation Support
Montreal QC
514-931-0841
abelanger@bdo.ca

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO Canada LLP to discuss these matters in the context of your particular circumstances. BDO Canada LLP, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO Canada LLP or any of its partners, employees or agents.

BDO Canada LLP, a Canadian limited liability partnership, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the BDO network and for each of the BDO Member Firms.

Copyright © January 2017 BDO Canada LLP. All rights reserved. Published in Canada.

www.bdo.ca

