



## CANADIAN DESIGN-BUILD INSTITUTE

---

400-75 Albert Street  
Ottawa, Ontario K1P 5E7  
Tel: (613) 236-9455  
Fax: (613) 236-9526  
www.cdbi.org

The Risk Management Committee of the Canadian Design Build Institute is pleased to enclose the following article which looks at and addresses employee fraud that can occur within construction site operations and operations as a whole. Although this article is applicable to operations beyond the Design-Build industry, we believe information and advice was relevant to all of our members.

The Risk Management Committee of the Canadian Design Build Institute will continue to circulate articles of this nature to members as they become available. We trust this will be found to be of interest and beneficial.

### **EMPLOYEE FRAUD: KEEPING THE "F" WORD OFF YOUR CONSTRUCTION SITE**

by David Miachika, Ross McGowan and Robert Dawkins  
Borden Ladner Gervais LLP

#### **What is Fraud?**

Fraud is one of those words that all people seem to know and use but few seek to clearly define. It encompasses a broad category of deceptive behaviour designed to benefit the fraudster, or a third party, to the detriment of the target of the deception. Its scope is limited only by the ingenuity of people looking for the easy dollar.

The construction industry, like all others, is susceptible to fraud. Fraud may occur in the office or on the construction site and be committed by employees, external contractors, sub-contractors, professional service providers or other third parties. Fraud occurs where there is motive and opportunity. As a result, when business is booming you may be most susceptible, only to discovery when there is a market downturn, and you look closer at the books, that part of your profits have been walking out the back door.

When an employee fraud is discovered it is common for an employer to want their pound of flesh. There will be anger, hurt, outrage, and calls for retribution. This creates a difficult situation, as dealing with allegations of employee fraud requires a cool head, prompt action and a fair and thorough investigative process. The implications of using the "F" word can be serious and as such it is important that it be understood and cautiously used. Unsubstantiated allegations of fraud can do great damage to one's reputation, both to those making the allegations and those who are targeted, give rise to legal claims for defamation against those making the allegations, and, in the employment context, cause irreparable damage to long-standing relationships of trust and undermine employee morale.

The focus of this paper is to provide an overview of issues relating to employee fraud, including common employee schemes, means of preventing fraud, identification of fraud loss, and strategies for recovery. A comprehensive review of this subject is beyond the scope of this paper and employers are encouraged to seek fact specific legal and professional advice to



ensure prompt and effective action that minimizes their legal exposure and maximizes recovery if and when an employee fraud is discovered or suspected.

### **Schemes to Watch For**

Employee fraud is perhaps the area of greatest danger to all organizations, and it is estimated to account for 60-70% of business losses due to fraud.<sup>1</sup> Every organization suffers from employee fraud to varying degrees and, for so long as we place any trust in others to diligently carry out their duties for the benefit of a principal, there shall be employee fraud.

There are a number of means by which employees may defraud their employers. Common schemes include:

- **Embezzlement:** where funds are stolen from the employer and accounting entries are created in the financial system to cover up the theft;
- **Expense report fraud:** including submission of duplicate invoices, credit card receipts, and credit card statements to obtain multiple recoveries of the same expense, use of business credit cards for personal purchases, purchase and submission of expenses for which refunds are subsequently obtained by the employee, altering of expense receipts, submission of fictitious receipts, submission of receipts paid for by others, submission of receipts for personal expenses;
- **Payroll Fraud:** this may be accomplished through payment of salaries to ghost employees who are either fictitious or no longer ought to be on the firm payroll, inflated hours, manipulated deductions for employee withholdings, unusual lump sum payments, unauthorized payroll advances or employee loans which go unpaid;
- **False or Inflated Supplier Invoices:** submission of false invoices for suppliers who have not provided any goods, materials or services, or inflating invoices beyond the value received. Employees may submit invoices for businesses owned and operated by them to collect the funds as "phantom contractors", or they may work in combination with real suppliers who pay them a percentage of the funds paid out on fraudulent or inflated invoices;
- **Secret Commissions and Kickbacks:** suppliers provide "perks" to an employee so that they may receive or maintain business with the employer. Perks may include, gifts, cash payments, travel, lavish entertainment, payment of consulting fees or future benefits; and
- **Inventory or Asset Misappropriations:** where the fraudster steals, misuses or converts to their own use a firm's assets. This may be done through theft of inventory, equipment or materials, off-book sales, use of corporate assets for personal business, or skimming.

### **Identification and Prevention of Employee Fraud**

Fraud flourishes in an environment where there is both motive and opportunity. Motive is usually fueled by perceived need, mistreatment by an employer or greed. Opportunity arises because the victims of fraud have the assets, income or resources desired by the perpetrators and have failed to take all possible steps to prevent fraud, have misplaced trust, or have been lured by their own desire for gain.

---

<sup>1</sup> The Law Society of British Columbia, *Fighting back against fraud – a dark and shifting landscape*, Benchers' Bulletin, 2005: No. 5, November-December; PriceWaterhouseCoopers, [Global Economic Crime Survey 2005](http://www.pwc.com), available online at [www.pwc.com](http://www.pwc.com).



Many internal and external frauds go on for years without detection. Organizations that have not given much thought to fraud rely on the knowledge of their employees and trust with little more to monitor or detect unauthorized activity. Larger firms sometimes mistakenly assume that auditors will detect and warn of such problems, all the while, putting the task of cheque reconciliation to either the 'helpful hard-working and trusted employee' or alternately doing the reconciliation once a year to give to the accountant for taxes. If fraud were so easily identified it would be far less likely to occur but, unfortunately, it is not so easily spotted.

## **Fraud Identification**

The typical perpetrator of a fraud may not meet with typical expectations. Fraudsters are likely to appear to be honest and trusted employees having the following traits:

- Long term employee;
- Position of trust;
- Works long hours;
- Works quietly; and
- Rarely takes vacation or takes very short vacation.

Perpetrating and covering up a fraud requires dedication and the perpetrator will not want to draw attention to him or herself. The commonalities of the fraudulent and dedicated employee make the task of fraud prevention a challenging one but there are some indicators to watch out for, including employees:

- Living beyond their means;
- Changes in personal circumstances;
- Emotional instability;
- Addiction problems;
- That see "beating the system" as an intellectual challenge;
- Dissatisfied with their job; and
- Perceive themselves as being underpaid.

While internal controls can assist in reducing exposure and increasing detection, frauds are usually undertaken when employees spot and exploit weaknesses in internal systems or during periods of turmoil, such as high employee turnover or extremely busy times, which make it more difficult to effectively implement prevention policies. The fact is that the single most effective means of detection is employee tips at 26.3%, followed by detection by accident at 18.8%.<sup>2</sup> Other means of detection contribute as follows:

---

<sup>2</sup> The White Paper, Topical Issues on White Collar Crime: "2002 Report to the Nation on occupational Fraud and Abuse": Association of Certified Fraud Examiners; May/June 2002, Austin, Texas.



<b>Method of Detection of Frauds</b>	<b>Percentage of Cases Discovered</b>
Tip from Employee	26.3
By Accident	18.8
Internal Audit	18.6
Internal Controls	15.4
External Audit	11.5
Tip from Customer	8.6
Anonymous Tips	6.2
Tip from Vendor	5.1
Notification by Law Enforcement	1.7

The implication of these findings is that an effective 'Tip Line' coupled with strong internal controls provide the key to detection of internal fraud. Legal counsel should be involved in developing 'Employee Fraud Policy Statements and Conflict of Interest Guidelines' for the education and assistance of employees. Such policies provide a means of promoting core values, honesty and integrity and introducing detection and reporting policies to employees at the outset of employment. Through the course of employment, employers should take steps to re-affirm the concept that employee fraud is more than just taking from the employer; it is stealing a little part of the trust, independence and responsibility that we each strive for in our respective sphere of employment. Those employees that are bilking the system are in essence taking from us all and are creating an environment in which it is less desirable to be. Similarly, strong internal controls start at the top. Corporate governance therefore will set the standard by which the rest of the organization measures its entitlements.

### **Prevention of Fraud**

Numerous studies have identified that in a typical population, approximately 15% of people are scrupulously honest and will not steal, about 15% of people are notoriously dishonest and will actively pursue opportunities to steal and the remaining 70% are influenced by a combination of opportunity, quantum at issue and risk of detection. That 70% in the middle can and are swayed by extraneous factors such as observation of corporate governance of senior management, promises of fidelity, clear corporate policies, perceived risk of detection and consequences arising from detection. While no policy can completely prevent employee fraud, this 70% is likely to be influenced by strong fraud prevention policies.

Prevention of employee fraud requires regular consideration of operational risks and continuous development of policies and controls designed to ensure: (a) hiring of honest people; and (b) keeping people honest. While no internal controls can completely eliminate fraud risk, such policies can reduce exposure, foster reporting of suspicious activity by employees and assist in early detection of fraudulent schemes. Some examples of prevention policies are reviewed below.

### **Know Your Employee**

While no degree of due diligence at the stage of hiring can completely eliminate fraud, a goal at this stage is to try to filter out the 15% of people who are notoriously dishonest and will actively pursue opportunities to steal. These people may have been caught before and discovery of a checkered past may well be as easy as a phone call or Internet search away. The key at this



stage is not only to verify previous employment and education of employees but also to assess the financial stability and security risk of prospective employees.<sup>3</sup>

Incorporating some or all of the following into your practices can help to increase the odds that you hire honest employees with lower motivation to commit fraud:

- **Require a résumé from all applicants:** Obtaining a written résumé will assist you in identifying issues which may not be immediately apparent if only a verbal interview is conducted. In particular, gaps in employment should be immediately apparent and you will have an opportunity to obtain an explanation from the applicant. While there may be an innocent explanation, gaps in employment may also be indicative of problems with previous employers.
- **Check References.** Obtain references, preferably at least two, from all applicants and be sure to contact them. Past employers may be reluctant to expressly advise of allegations of fraud against a former employee for a variety of reasons but a past employer is unlikely to positively endorse a former employee suspected of committing fraud.
- **Obtain Consent to Obtain a Credit Report.** A credit bureau report may include information about legal claims against a prospective employee that have gone to judgment. It may also show whether the employee is in dire financial straits and likely to have a high motivation to commit fraud. Prior consent must be obtained to obtain these searches in British Columbia. You must have evidence of such consent and as such, written consent should be obtained and placed in the employee's personnel file.
- **Other Searches.** For employees who will be in a position of financial responsibility it may be worthwhile conducting other background searches. Such searches could include court registry searches for judgments obtained against them or outstanding actions or bankruptcy searches. Even a simple step such as Google searching a prospective employee could uncover a past fraud.

### Internal Policies and Controls

Establishing strong systems of internal control increases the likelihood of detection. Such controls will also increase the psychological risk associated with committing a fraud and may act as a deterrent. Common internal controls that can be implemented include the following:

- **Division of Duties.** Be sure to separate the three key functions of authorizing transactions, collecting or paying money, and maintaining financial records. One employee should not have responsibility for both sides of an office function such as preparing cheques for payment and reconciliation of that bank account, or preparing payroll cheques and maintaining the payroll/employee record system. By dividing responsibility you reduce the ability of any one employee to commit a fraud and increase likelihood of detection.
- **Mandatory Vacation.** Require that employees take vacation at least annually. This will allow other employees to sit at the desk of key employees and see how they carry out their operational responsibilities. This makes it more difficult to keep fraudulent transactions under cover.

---

<sup>3</sup> While a review of privacy law is beyond the scope of this paper, Employers should consider implications of privacy legislation such as the *Privacy Act*, R.S.B.C. 1996, c. 373, in collecting, storing and using employee personal information. Violation of employee privacy rights can give rise to claims for damages.



- **Obtain Original Documents.** Insist on having original invoices available to the cheque signor at the same time cheques are signed and have the signor note in ink on the invoice his or her name, the date, time and cheque number used to pay the invoice or group of invoices.
- **Reconciliations.** Perform reconciliations of accounts at least monthly, in particular bank reconciliations. If you prepare budgets and forecasts, compare the budget against actual revenues and expenses and investigate any discrepancies.
- **Outside Accounting:** Consider using a reputable external service provider to provide a payroll service and look after payroll accounting.
- **Outside Reconciliations:** Periodically have someone different reconcile your bank statements (such as an employee of your external accountant) or at least a different employee. Periodically have a person other than your bookkeeper pick up and review cancelled cheques before delivery to your bookkeeper.
- **Outside Reviews:** Consider having an annual "spot audit" by your accountant that is held without notice to the organization.
- **Supplier Controls:** Know your suppliers and consider implementing a list of approved suppliers. This will ensure that you know who you should be receiving invoices from.
- **Restrict Access to Company Cheques and Banking Documents.** Access to software used to generate company cheques, hard copy cheques and banking documents should be restricted to necessary persons and be password protected or kept in locked premises or cabinets.
- **Construction Site Controls:** On site controls should be implemented to protect against theft and conversion of material and equipment. Protective steps may include "spot" inventories of equipment and materials and reconciliation of inventories against supplier invoices. On site equipment and material deliveries should be monitored and documented to facilitate detection.

While implementing controls such as the foregoing may help to reduce and identify fraud, perhaps the most effective means of reducing fraud is to ensure that employees feel valued and that they have a personal stake in the success of the employer's business. Cultivating a reputation of fairness by treating personnel fairly, paying equitable salaries, listening to employees, and recognizing and reinforcing good work can go a long way to reducing fraud. If employees feel like cheating the company is cheating themselves they are far less likely to steal from their employer and far more likely to report the misconduct of their co-workers. The policies outlined above can work in combination with these efforts by creating opportunities for employees to identify and report fraudulent conduct in the organization.

### **When to Use the "F" Word – Investigating Allegations of Fraud and Employee Confrontation**

Where employee fraud is suspected or tips are received, a number of issues arise with respect to how best to investigate and respond. This section provides an overview of some common issues to consider at the investigation stage. The key to a good investigation is to keep the hypothesis of fraud open ended until sufficient evidence has been amassed to make the final supposition. The investigation can be treated as a very serious game of "Clue" where the stakes are always the reputation and good name of a previously trusted member of the team and the consequences of ill-founded supposition can be life altering for all concerned. Even after reaching an investigatory plateau, be prepared for assumptions and inferences to change, parties and persons to be added or implicated, evidence to be destroyed or altered and recoveries to be thwarted through perpetuation of the initial conduct.



If one receives tips or discovers irregularities which reasonably lead one to believe that an employee is stealing, procedures should be put in place to deal with such situations. The key goals at this stage will be to collect and secure all evidence of the fraud and ultimately confront the suspected employee and seek recovery. A detailed checklist of issues relating to employee confrontation is attached as Schedule "A" and a brief overview set forth below.

Before confronting or talking to the employee, the employer should obtain as much information as possible to prepare for the meeting. The employer should consider obtaining the assistance of their professional consultants. This would include your lawyer (for employment issues, issues concerning possible defamation, combined with issues needed to direct a fraud investigation) and possibly Forensic Accountants.

When a business discovers a loss, it is important that one person in the company be responsible for the collection and protection of any evidence, documentary or otherwise. Have the evidence placed in a secure place and restrict access to it. This includes computer hard-drives and other relevant electronic storage devices.

**DO NOT WRITE ON OR MARK THE DOCUMENTS IN ANY WAY.** If one must make notes on the document make a photocopy of it and write on the photocopy. If one wishes to mark the documents for identification purposes do so on the back of it where it does not deface the original. Inappropriate markings on documents complicate the use of the document in either civil or criminal proceedings.

When the employee is confronted, it should be done with a minimal number of persons in the room. It is recommended that there be no more than two people other than the employee (one to run the confrontation meeting and one witness). During the course of the meeting, the interviewer is deemed to be a person in authority and one's approach therefore becomes very important if you wish to use what the employee says at a later date for either Criminal or Civil proceedings.

During the meeting, one must be careful not to give any inference that unless the employee tells you what has been going on you will go to the Police. Threatening to report or reporting the matter to the police cannot be contingent on what the employee does or does not say. Giving this inference can affect using this information at a later date and may expose you to a claim or charges for uttering a threat.

When meeting with the suspected fraudster, care must be taken not to do anything that may prejudice a potential claim or the Insurer's position (if a fidelity policy is in place). If a business intends to advance a claim under its insurance policy, then the insured should be working in concert with the Insurer from the beginning and refrain from taking any steps without prior consultation.

When the suspected fraudster is interviewed, in addition to the facts of the suspected loss, the interviewer should also try to obtain information in relation to assets and collateral income sources of the employee. This will prove valuable information in seeking recovery.



## **Recovery of Fraud Loss**

Initial pursuit of recovery is an important part of virtually all internal and external fraud losses. While this paper does not delve into all issues of recovery, it is worthy of note that recovery issues are complicated by the fact that settlements will inevitably be broken, assets will be hidden and claims through to trial are both rare and costly. Recovery efforts must usually be based on ingenuity rather than standardized pursuit of a legal action similar to a debt recovery claim.

Consideration should be given to immediate negotiation of settlements with employee fraudsters. In many cases, employees will be quick to seek closure, even if they are not then able to actually make full restitution. The terms of any settlement should be carefully crafted to address concerns that may be raised by insurers, trustees in bankruptcy, and other creditors who may wish to assert fraudulent preference claims in attack of the settlement. Admissions of the fraud are also key, to provide maximum likelihood that the settlement will survive bankruptcy.

Court proceedings are also an important element of many recoveries and the remedies of Mareva injunctions (asset-freezing orders) and Anton Piller orders (search orders) can be extremely effective tools to preserve funds for maximal recovery. An employer should be sure to retain legal counsel with special expertise in the area of fraud recovery, approach the process with an open mind and consider creative compromises.

Alternate sources of recovery should also be investigated in every case of fraud, including possible claims against auditors for failure to detect, against external parties complicit in the fraud, or third parties who benefited from the employee's fraudulent conduct. While in many cases these alternative claims do not survive scrutiny, each case will depend on its facts, and in fraud, many of the facts are known only to the fraudster.

## **Conclusion**

Employee fraud is something that will always be with us. It is an unfortunate cost of entrusting responsibility to others. This said, the risk of fraud must not be allowed to poison the work environment or interfere with effective business operations. Employers should adopt the policy of "trust but verify", implementing policies to divide key responsibilities amongst different employees and to create opportunity for detection. Fraud risk cannot be eliminated but putting appropriate screening and control policies in place can diminish it.

With this in mind, every investigation and prosecution of fraud should end with a review of the circumstances that have allowed the fraud to occur. It brings to mind the adage: "Fool me once, shame on you. Fool me twice, shame on me." Fraud is a crime of opportunity and it seeps into the cracks of an organisation's systems and policies, like rainwater probes the surfaces of a leaky Condo. If the organisation was poorly designed or is poorly maintained, it will get in and begin its rot soon after. However, even the best roofs will eventually leak and even the best organisations will eventually fall victim.



### SCHEDULE "A"

	Date Done	By Whom
<b>Pre-Meeting Preparation</b>		
1. Secure suspect employee(s) personnel file.		
2. Secure relevant company documents to investigation.		
3. Ensure that investigation is on a "need to know" basis identifying only those senior management persons with information concerning the investigation. If other input is required, such input should be only as is required without identifying the nature of any accusation directed at any employee in particular.		
4. Contact legal counsel to discuss coordination of timing, location and persons in attendance for meeting(s). If employee is a member of union, review collective agreement for rights of shop steward/Union representative attendance.		
5. Prepare copies of documents relevant to investigation and organize as appropriate.		
6. Consider potential reaction of employee(s) (both employee under investigation and other staff) and determine whether counseling for employee(s) should be offered.		
7. Prepare outline of known facts for review with suspect employee(s).		
8. Identify all security concerns with respect to suspect employee(s) including keys to premises, pass cards to premises, passwords to network system, voice mail, e-mail, data stored on laptops, data stored on home computers, access rights from external computers, possible Trojan horse access, banking arrangements, dealings with outside suppliers, and any other source of vulnerability between suspect employee and company.		
9. Consider whether employee fraud triggers fidelity insurance coverage or duty to give notice to insurer or regulatory authorities and if so, take appropriate steps to give notice with assistance of legal counsel.		
<b>Meeting with Suspect Employee</b>		
1. Identify senior management to attend at meeting (include person in charge of investigation, senior management with responsibility for human resources, and if appropriate, outside legal or other consultants).		
2. Schedule meeting for time and location to accommodate prospective length of interview and further steps as may be required following interview. Consider whether off-site location appropriate to avoid embarrassment or unpleasant scene.		
3. Conduct interview of suspect employee(s) and request explanation. (If more than one employee is under suspicion conduct separate back-to-back meetings.) Record notes of explanation provided by employee(s) on confrontation of matters at issue. Do not tape record conversation unless done with knowledge and consent of employee.		



	Date Done	By Whom
4. Inform employee(s) of duty to investigate and re-examine explanation offered by employee with documents as compiled prior to employee meeting and invite further explanation of specific instances from employee.		
5. On review of suspect employee's explanation, consider whether any disciplinary proceeding should be pursued including: (a) explanation accepted and no further disciplinary conduct warranted; (b) letter of warning; (c) written acknowledgement of wrongdoing by suspect employee with commitment to avoid such future conduct; (d) suspension with pay pending investigation; (e) suspension without pay pending investigation; or (f) immediate dismissal. (Note that suspension of employee may amount to constructive dismissal and any decision in that regard should be done with advice of legal counsel.)		
6. If further investigation is warranted following employee meeting, temporary steps should be taken to preclude further access to company facilities by suspect employee while investigation is underway, including request for keys, pass cards, passwords, and any other security concerns as referenced above.		
7. Consider whether appropriate to request that suspect employee access office computer and provide all passwords for access prior to departure. Consider whether appropriate to request hard drive dump of laptop or home computer and deletion of company files located on other computers.		
8. If employee is suspended, inform employee of duty to assist with ongoing investigation, confidentiality of the investigation, and consider whether appropriate to offer counseling to employee.		
<b>Post-Meeting</b>		
1. Pursue any further investigation required.		
2. Consider possible further interview of suspect employee prior to termination.		
3. If employee was in sensitive financial position or otherwise had access to banking records of company or cheque signing authority, take steps to revoke as appropriate and if necessary. Likewise if employee had relationships with outside suppliers or customers consider whether any contact should be made to those parties, and if so, the nature of the information to be provided. Consider also whether outside suppliers may have conspired with suspect employee. (Note that no allegations of dishonesty should be made about the employee at this stage.)		



	Date Done	By Whom
4. Consider possible terms of agreement as between employer and employee concerning disengagement, and if loss suffered due to fraud, consider maintaining rights of claim in fraud subject only to release if restitution made in full. Any settlement agreement should further be premised upon a representation and warranty by the employee as to the scope of fraud. Consider whether insurer should be involved in settlement agreement. Obtain legal advice on terms of any agreement before it is finalized.		
5. If employee is to be terminated, take appropriate steps to permit employee to recover personal items and take inventory of work area.		
6. Have meeting notes transcribed and forwarded to counsel for legal advice concerning possible claims for wrongful dismissal/ recovery.		
7. Consider review of company systems including hiring, supervision, accounting, internet access, banking, etc. to address possible shortcomings and prevent further similar losses. Consider purchasing fidelity insurance for coverage against future losses. Consider implementation of Employee Fraud/Dishonesty Policy.		
8. Consider consulting with legal counsel to review possible claims as against employee or others for recovery.		

Note: The checklist set forth above is not intended to be legal advice to cover each specific situation but is provided as a general outline touching upon many of the common areas faced with investigation of possible employee fraud. It is recommended that this checklist be used as a starting point and that employers address such other issues as are particularly relevant to their organization's needs and to seek specific legal advice with respect to individual circumstances that may involve employee fraud.

Borden Ladner Gervais LLP is among Canada's most respected full-service national law firms. With more than 700 lawyers, intellectual property agents and other professionals in six offices across the country, BLG provides corporate, litigation and intellectual property solutions to a wide range of clients nationally and internationally.

David L. Miachika, P. Eng., is a partner at the Vancouver office of Borden Ladner Gervais LLP and is the Regional Leader of the Construction, Engineering, Surety & Fidelity Practice Group. Mr. Miachika was admitted to the British Columbia Bar in 1989. He is a graduate of Dalhousie University Law School with a Bachelor of Laws in 1988. Prior to that, he received a Bachelor of Applied Science (Civil Engineering) from the University of British Columbia in 1981 and is a registered Professional Engineer in BC since 1984. Prior to obtaining his law degree, he worked for several large general contractors as a project manager on commercial, industrial, marine and heavy civil construction projects. Mr. Miachika's legal practice is exclusively in the area of dispute resolution for commercial litigation and arbitration, primarily focussed on construction, surety, insurance, engineering, builder's liens, environmental, condominium and real property disputes.

For further information on David Miachika or Borden Ladner Gervais LLP and their services, please visit [www.blgcanada.com](http://www.blgcanada.com),