FINANCIAL ADVISORY

Ten Ways to Protect Your Business from Fraud

December 2015

According to the Association of Certified Fraud Examiners (ACFE), the typical organization loses about 5% of its annual revenues to fraud. The average fraud scheme costs an organization approximately $150,000 annually and over 50% of cases have no recovery of losses.

BDO's Rosanne Walters, who specializes in forensic and investigative services, offers these tips:

1. Know your employees:

- Perform proper screening of your employees, including criminal checks and due diligence regarding the employee's background.
- Look into gaps in employment and anything that does not add up in a resume.
- A two-year gap in a resume could mean jail time, as was the case with a company that recently discovered their employee had been imprisoned for embezzlement six years prior to being employed. It was a difficult ethical decision for the employer once this information came to light because the gap existed on the resume but the employer never asked about it and did not perform a criminal background check.
- It is not uncommon for resumes to contain false information. Outside services perform resume checks for a very reasonable fee.

2. Protect your information:

- Protect your business from cybercrime with firewalls, anti-virus programs, passwords and controls for employees working outside the office on personal computers. Remember that information can be removed easily from office computers by portable memory drives and using email.
- Protect information shared on social media sites. Train employees about the dangers of sharing personal information that can lead to fraud.
- Be aware of information stored on the hard drives of photocopiers and cash registers. Purge information on a regular basis or save offsite in a secure environment.
- Recently, a construction company lost all of its data when the office manager resigned. This confidential information included bidding processes, financial information, pricing strategies and costing information. The information was removed by email to the employee's personal email account, prior to resigning. After resigning, it was discovered that the employee went on to join a competitor.

3. Start a confidential reporting system:

- Allow others to watch and report by starting a confidential whistleblower program.
- According to the ACFE, 42% of fraud is detected by tips from employees, customers and suppliers.
- Most employees intuitively know when behavior appears suspicious, but they usually have no confidential method of reporting the situation.
- Expediting confidential reporting can be as easy as setting up a separate mailbox on your phone system for complaints, in addition to advertising and encouraging reporting later on.
- In one recent case, a property management company discovered that their property manager accepted bribes to approve non-qualified tenants, when one of the tenants complained.

4. Protect your business from fraudulent third parties:

- Perform due diligence of third parties involved in your business, including property managers, contractors, sub-contractors, venture partners, suppliers and consultants.
- Find out who these people are and whether their business is reputable and legitimate.
- Is the third party real? Are you paying for services that either do not exist or for which you are over-paying?
- Obtain bids for services as often as possible.
- For example, a real estate company paid for painting services, but the services were performed elsewhere and billed fraudulently to the company.

5. Be aware of corruption schemes:

- According to the ACFE, the most common schemes in Canada involve some kind of corruption, such as accepting bribes and/or kickbacks.
- Kickbacks can occur when you unwittingly overpay a supplier and the supplier splits the overpayment with another stakeholder.
- Be aware of what services are being performed and the market rate for these services. Kick-back schemes occur more often when you are over-paying for services.
- Be aware of relationships between third parties and insiders.
- One company paid for the services of an electrician who was overcharging for the work performed and then splitting the difference with the property manager for a sizable kickback.

6. Look at your bank statements:

- Many embezzlement schemes occur when an insider has access to a bank account or cheques.
- Cheque tampering schemes are very costly and can be as simple as altering company cheques after they have been signed. Review all cheques when they come back from the bank to confirm that they match the originals.
- Another common occurrence is when employees pay online for personal bills and retail purchases using company's funds. Regularly check your bank balance for discrepancies.
- In one situation, a bookkeeper submitted a cheque for signature intended for a legitimate supplier. Once the cheque was signed, the bookkeeper destroyed the cheque and recreated one for the same amount, only this cheque paid her personal VISA bill; the funds never made it to the supplier.

7. Scrutinize expense reports:

- Expense account fraud is very common in all businesses.
- Expense reports should be supported by original receipts before submitting for review and approval.
- Some employees submit personal expenses and even multiple reimbursements of the same expenses, without incident.

8. Know what assets you are buying and how they are being used:

- Assets sometimes grow legs and walk out the company front door due to theft or by items deemed to be borrowed.
- Keep track of assets at all times.
- Install video cameras wherever possible.
- One company work site housed heavy equipment which was used regularly by the company's manager. The company manager personally saved himself the cost of buying, insuring and maintaining his own equipment because he fraudulently used his employer's.

9. Use a payroll service and check that employees being paid are real people:

- Payroll schemes can be a big threat to any organization.
- Employees can overcharge for hours they did not work or, even worse, a company that is not paying attention may be paying for employees who are not working at all.
- For example, a business continued to pay for a departed employee's salary because there was no one in place to oversee and/or perform employee exit interviews.

10. Establish a good code of conduct:

- Establish a good code of conduct for your employees and third parties.
- Set out your expectations on what constitutes acceptable behaviour.
- Review these policies with your employees on a regular basis, including annual sign-offs to be placed in an employee's personnel file.
- Obtain fidelity insurance for employee fraud and theft to cover the unexpected.

About Rosanne Walters:

Rosanne Walters, CFF, CPA, CA, CBV, CFE is a Partner with BDO's Forensic and Investigative Services group. You can reach her at 604 646 4381 or rwalters@bdo.ca.