BROTEMARKLE, DAVIS & CO. LLP

Putting People First

Think you're too small for fraud? Think again.

As we begin a new year, there is much hustle and bustle. We're in the midst of short- and long-term planning and budgeting. We're busy checking our equipment to see that it is properly serviced and ready for the new season. We're rushing to get our accounting records in order to meet our year end tax filing requirements, and we're trying to finalize the information needed by banks and other government agencies.

In all of this chaos, who has time to consider if we are doing everything we can to reduce our company's exposure to fraud?

In fact, very few small businesses **ever** take the time to consider where they might be vulnerable to fraud. These businesses think "we are small enough that fraud won't happen to us".

Research performed by the Association of Certified Fraud Examiners (www.ACFE.com) found that small businesses (those with less than 100 employees) have the greatest frequency of fraud of all organizations, representing 38% of all fraud cases, with their median loss approximating $200,000.

The beginning of a new year is the perfect time for small businesses to ask themselves these questions:

1. Can we survive if fraud occurs within our company?
2. How can we reduce the threat of fraud?

Three factors (known as the Fraud Triangle) need to be present in order for fraud to occur:

- **Opportunity** - there is a way to misappropriate company assets.
- **Pressure** - there are financial or social events that make the employee feel the need to perform a fraudulent act.
- **Rationalization** - there is a way for an employee to justify their actions so they do not feel that they are unethical or wrong. Either they feel they deserve a reward or they sincerely plan to reimburse the company when events in their life improve.

If you can reduce or eliminate any of these factors, your company's fraud risk will decrease significantly.

Here are some ways to reduce your exposure to fraud:

1. **Communication –** Talk to your employees. By communicating with your employees you can learn a great deal about what is currently happening in their lives, and become aware any significant changes (external pressures) that could tempt them to commit fraud.

2. **Control the bank statements –** Have bank the statements sent directly to you unopened. It is highly recommended that every business owner have bank statements mailed directly to their home. Being the first person to examine the bank statements and returned checks does a number of things to help reduce the threat of fraud. First, the practice creates the perception that you are watching what's happening in your company. Secondly, by looking at the bank statements, you will be able to see any unusual activity on a timely basis. But, you need to do more than just review the bank statement. You should also randomly select transactions from the statement(s) and inquire about them to obtain a greater understanding or reminder of what took place. The process of asking questions will further reinforce the idea that you are closely monitoring all of your company's activity.

3. **Segregate as many duties as possible –** Giving one person too many duties can increase the likelihood of fraud. Segregating employee duties and creating oversight Examples can be as simple as having one person review the work of another. Having a reviewer makes it difficult for an employee to hide fraudulent activity. This practice can also serve to reduce the rationalization that has a tendency to occur with long time employees. When an employee has been with a company for many years, it is not uncommon for them to begin to feel left behind, making it easy for them to rationalize the misappropriation of company assets. In summary – when it comes to employees, trust but verify.

4. **Lock and protect your valuables –** Make sure that your unused checks are being properly stored. Leaving blank checks lying around the office makes it easy for someone to slip one in their pocket. Banks don't always verify signatures and with today's technology, it is fairly easy to scan and print a signature on a check for cashing. Also make sure that you regularly inventory your movable fixed assets; these can sometimes wander offsite and be sold on internet auction sites like "EBay".

5. **Request supporting documentation –** When you are given checks to sign, ask to see the source document. You should develop a policy and habit of always matching supporting documentation to checks before you sign them. This practice will help ensure that your company records are accurate - that the check amount agrees to the invoice, that transpositions have not occurred, that all available discounts are taken, and that the name on the check agrees to the invoice.

6. **Develop a written code of ethics and enforce a zero fraud tolerance policy – Have a policy and enforce it.** Take corrective action as soon as fraud is discovered. Regardless of the perpetrator or their level in the organization, corrective action will set a precedent and establish an expectation that other employees should help deter fraud. Fraud can multiply if it is not dealt with as soon as it is discovered.

7. **Hold annual meetings** – Meet with all employees at least once a year and remind them of company policies. Encourage people to come forward if they suspect suspicious activity. Share information about your whistleblower policy. You can allow employees to anonymously report activity by creating a fraud hotline or by placing locked boxes around your facility. Employees can anonymously deposit letters in these boxes for collection by the owner.

8. **Expand employee prescreening –** Many small companies do not allocate sufficient resources to the screening process for hiring new employees. Often when someone is terminated from their place of employment, they will have a tendency to leave that position off of their resume. You need to be careful to watch for employment gaps and to obtain an adequate explanation for the gap. You should contact the previous employer inquiring why there was a termination of employment to see if their explanation agrees with your interviewee. (Be sure to investigate the rules for employment law before asking any questions regarding candidates.) Also look at social-networking sites on the internet for characteristics of the perspective employee, people are posting events of their private lives on these sites with little regard for who might read them. If possible, perform a background check.

   Current popular social-networking sites are:

   - Facebook.com
   - Myspace.com
   - Twitter.com
   - Youtube.com
   - Flicker.com

9. **Promote strong leaders –** Strong leaders promote strong employees. You don't want to risk promoting a poor leader who does not demonstrate character and integrity; he will lead employees to do the same. A strong employee with high values and a commitment to the company will encourage those around him to follow his lead.

10. **Treat your employees well –** If your employees are happy, they will be less inclined to commit fraud and they will be more willing to report suspicious activity. A simple thank you and gesture of appreciation can go a long way towards earning an employee's trust and respect.

An employee is a person working for the benefit of the company. Fraudsters are self-employed people working for their own benefit at the expense of the company.

If you would like more information on how to prevent or detect fraud within your company, please contact BDCo LLP:

- Phone – (707) 963-4466
- Email – Craig@bdcocpa.com or Sam@bdcocpa.com
- Visit our website – www.bdcocpa.com