pro@ctive™

To: Clients, Associates & Friends of Pro@ctive CPA
From: Mark Wyssbrod, Managing Member
Date: August 21, 2011
Re: The "F" Word In Your Business

The "F" word is a sinister word and should not be used in the normal course of one's day. However, society has evolved and seems to be using the "F" word more often, perhaps daily. What sort of moral and ethical dilemma does this pose when we "F" this and "F" that? The "F" word I am referring to is FRAUD!

We are surrounded by fraud in all parts of our lives! Our investments are not as safe as we want them to be, think Enron; nor are our small businesses. That's right! Fraud has infected both Wall Street and Main Street. It does not discriminate on size, economy, industry, creed, religion or race. But apparently, men do commit fraud more than women (57% to 43%). As long as the economy stays in challenging times and individuals want to live outside of their means, fraud will continue to be a part of our business environment.

Who commits fraud? Any individual with opportunity, incentive or pressure, rationalization and capability is candidate for committing this crime. You might believe economic environment should be this list. However, fraud occurs in good times as well as in bad times. Enron occurred in what was believed to be a stable economy. However, more challenging times do add pressures to individuals to rationalize their acts.

The opportunity for misappropriation of company funds is possible due to minimal or lack of internal controls. As reported on May 15, 2011, 72% of the member of the International Account Payable Association stated fraud is on the rise in the back offices of business. Incentive to misallocate company funds is due to compensation pressure, personal lifestyle or the fact only 25% of frauds which were detected were publicly reported. Individuals rationalize their actions by saying it is a loan they will repay (but never do) or they are underpaid or for the extra hours they worked or they just plain deserve it! Finally, every human being is capable to commit this sinister crime.

Fraud doesn't have a face or a smoking gun. We will focus on who and how fraud is committed in the small business arena. First, studies have reviled that it not just the bookkeeper involved with stealing from the company. Any one in small business who is trusted is qualified to commit tempted acts of self-interest. Be careful, for an old saying is "fraud and stupid often look the same".

Some of the most common schemes in small business are false invoicing, check tampering and inventory. A false invoice is when a manager who had the right to approve invoices approves fake invoices. This can include a fake company the manager creates, which does not provide any services or goods, and approving invoices, which allow current vendors to pad invoices in order for the manager to receive a personal kick-back from the vendor. If you do not believe this has happened to you, you have been had! Solutions include a controlled master vendor list in which a full due diligence is completed before checks are delivered. Additionally, you can use data mining software to review your information. For example patterns which can be symptoms of this disease include vendor amounts starting small and then increasing over time, but never above a manager's approval level.

The second of the most common schemes includes check tampering. Check tampering occurs when the accounting system says ABC was paid, but the physical check states your employee or another party was paid. You can minimize your exposure to check tampering by not just checking off the items in a reconciliation module, but matching check images to the reconciliation cash disbursement names, as well as amounts.

The next most common scheme is inventory theft. Inventory can be used as office supplies, time, or physical items for resale. A good prevention for inventory theft is time clocks, security cameras and regular, unscheduled, physical inventory counts.

Unfortunately, managers and auditors spend their time trying to determine who is stealing time and office supplies which are minor compared to the aforementioned schemes. Management and outside advisory should focus on the areas fraud is most commonly committed and with larger dollar amounts.

The number one fraudster out there is the small business owner, high ranking managers and officers. That is right! This elite group commits the majority of misappropriation of company assets. They do this through intimidation of employees (i.e. just do this or your fired) and surrounding themselves by advisors they threaten to fire if they don't report the answer they want to receive. Business owners might believe all of their company assets are their personal assets. This is incorrect for they have a fiduciary responsibility to the company. If they want the corporate assets, they need to distribute them officially.

You can try to prevent fraud by controlling the environment, having fraud risk assessments, conducting anti-fraud control activities, information and communication, monitoring and placing in key steps. The cost of one average fraud will be more than the cost of the preventive acts. Controlling the environment includes establishing the proper tone and example from officers and top managers, code of ethics, organization culture, fraud policy, a hotline for reporting fraud and a program to protect whistle blowers. If managers always have exceptions to rules, staff members will not respect or follow the internal controls either. An outside advisor caught less than 18% of fraud. The largest way to detect fraud was an anonymous tip hotline.

When was the last time you tested your internal controls? A small business should have a third party review their operations and establish a fraud risk assessment process. A simple test might be reviewing salaries and matching the car your employee drives to work. Can an employee with 2 children making $40,000 afford a luxury vehicle?

What are your accounting procedure weaknesses? Anti-fraud control activities define and link mitigating controls to identify risks, design and implement necessary preventative actions and place in position detective controls.

Have you ever communicated to your employees fraud will not be tolerated? Providing fraud awareness training and communicating regularly as well as promoting the importance of fraud detection and risk management is a vital action.

Monitor activities periodically by an independent evaluation of anti-fraud controls. Having an outsider look over your employee's shoulder every once in a while and ask the employee question after question forces the employee to think twice before attempting to commit an inappropriate act.

Key steps include properly addressing fraud risks within an organization through governance, risk assessment, prevention, detection, deterrence and investigation response.

In good economic times, and in more challenging ones, fraud can be committed. Small businesses cannot afford the losses associated with fraud. Now is the time to improve internal controls and anti-fraud measures.