

Fraud and Embezzlement in the Small Business Environment

Fraud and Embezzlement in the Small Business Environment By: Glenn Carniello, CPA We have all heard much about fraud in recent years as it relates to business. In the early 2000s, the news was filled with scandals involving fraud of various types. The mere mention of Enron and Worldcom, for example, is now virtually synonymous with the word fraud. Although these scandals involved very large, publicly traded companies, the fact remains that fraud occurs most often in smaller businesses. Further, according to the Association of Certified Fraud Examiners, the losses incurred due to fraud in the smallest businesses are 100 times greater than those incurred by the largest companies. According to the 2006 Report to the Nation on Occupational Fraud and Abuse by the Association of Certified Fraud Examiners, "The median [fraud] loss suffered by organizations with fewer than 100 employees was \$190,000 per scheme; higher than the median loss in even the largest organizations. Small businesses continue to suffer disproportionate fraud losses." In my almost twenty years in business, I have never seen the frequency of detected fraud and embezzlement as great as it is at this time in our business community. It's tough to know exactly why the frequency with which fraud is committed has increased. It may be due to tougher economic times or specific personal circumstances causing more people to steal. Whatever the case, this abundance of fraud-related activity has only shone a brighter light on the issue. Let's first understand what fraud and embezzlement are by definition. According to Wikipedia, fraud is "in the broadest sense; a deception made for personal gain." Wikipedia defines embezzlement as "the act of dishonestly appropriating goods, usually money, by one to whom they have been entrusted." One of the key reasons fraud can occur, and why it is more frequent and severe in the small business environment, is the root of a word in the embezzlement definition; trust. In the smaller business office we often entrust employees with more responsibility and greater authority because the financial resources do not exist to hire many people over which to spread the responsibility and authority. This situation leads to the classic "lack of segregation of duties" which is a critical internal control concept. This scenario is inherent in small businesses and small business owners are highly susceptible to fraud and more specifically embezzlement as a result. Also, this trust is earned over many years in some cases. It seems that in many of the cases we see, the person committing the fraud has been working for the owners for 10 years or longer. It is precisely in these relationships where the trust and authority is given far more than it should be because the comfort is so great with the familiar individual and any and all guards are let down. It is an unfortunate observation that these most trusted individuals are, in many cases, the ones who are stealing with both frequency and in large amounts over long periods of time. In my career, I have uncovered fraud and seen its effects both financially and emotionally on the principals of the business. The cost to small business is greater than the hard dollar cost of the monies misappropriated. The distraction to the business, its employees, owners and others involved with the business is costly in terms of lost productivity as well as the cost to replace a once trusted and valued employee. There is the cost of recruitment and training of a new person as well as, in many cases, the cost of aggregating information to provide to authorities for prosecution. It has been my experience that in many of these instances of fraud, the perpetrator is not prosecuted. I've heard many reasons for why prosecution is not pursued. These reasons include: remaining loyal to the individual due to what used to be a strong relationship, not wanting to hurt the person beyond the loss of their job, or embarrassment in being the victim of such a crime, among others. I would suggest that in certain scenarios, one has a duty to prosecute. When you are involved in a situation where there are multiple shareholders, you have a fiduciary responsibility to prosecute and file related reports in an attempt to recover corporate assets. In many of the situations I've seen, the embezzlement occurred in a company owned by one individual. In those cases, the decision comes down to a personal choice as there is no responsibility to other shareholders. However, the rights of creditors should also be considered if there is any question that the embezzlement could place the company in a position where repayment of debt becomes questionable. It is also important to note that prosecution is a good idea so that the record of the individual committing the crime becomes public record. This public record will be discoverable by future employers performing background checks. Some Ways that Fraud is Committed There are many ways fraud can be committed. Embezzling cash is most common, however misappropriating goods or engaging in kickback schemes also occur with regularity. Let's begin with a few methods used to steal cash from the company. If you Google "signature stamp for checks" you will find approximately 276,000 links in less than a quarter second. Many of those links are attempts to sell signature stamps for convenience while other links discuss the fraud associated with the use of signature stamps. I'm of the opinion that using signature stamps is a bad practice. We have seen many accounting personnel use the signature stamp to commit fraud. In fact, before the turn of this century, I had suspected a Controller of embezzling cash. I strongly recommended to the owner to get rid of the signature stamp. I had also led an effort to do work to determine whether fraud was, in fact, occurring. Later that year, we had built a file such that the Controller, who had been there for over 15 years, ended up confessing. This person called me in to the conference room and actually thanked me for taking away the signature stamp months earlier. As it turned out, despite loyalty to the family who owned the business, this person's personal financial woes (which included a spouse who had been out of work for 18 months) simply made the temptation to steal too great. This person did not want to steal from the business (and the family) however, they felt as if they had little choice. The Controller stole in a number of ways, but most notable was the use of a signature stamp in preparing unauthorized checks. We have also seen straight forgeries on unauthorized checks. In a more recent case, an accounting person was allegedly forging checks to fictitious companies they had established, as well as checks written to their own business. In this case the accounting person had been employed with the company for over 15 years; another trusted employee. In another case, the Controller, who had been in that role since the Company's inception over 10 years ago (and with the management 4 years prior, for a total relationship of over 14 years) was the sole authorizing party for electronic funds transfers and to authorize payroll disbursements for the Company. This person was modifying their payroll, including

expense reimbursements on their paycheck and then to cover the trail, was doing journal entries to reclassify the amounts out of payroll and into indirect job costs, essentially spreading the stolen money over all the jobs in progress. The bank was preparing certain reports that actually highlighted the activity, however those reports were also sent directly to the Controller, who in turn destroyed the reports upon receipt helping to cover a trail in the short term. A few years prior, a large subcontractor client hired a new President. Upon reviewing the financial reports approximately 6 months after taking on this new role, we noted that materials were costing 51% of contract revenues. The concern we raised was that, historically, we noted materials to run approximately 37% of contract revenues. During an all-hands meeting with the Owner, President, Controller as well as one of my Partners, we asked the President to explain the increase. Instead, we were provided a quick, meaningless response and the President proceeded to move down the rest of our report for the next 20 or so minutes explaining variances in other areas. When it concluded, I again asked for explanation with regard to the increase in materials. The President's face and neck literally began to get blotchy, and, sweating profusely, asked for some time to take care of a skin condition they were dealing with. This President had given himself huge raises within the first six months in that role, and was demanding equity in the business prior to this meeting. Within a month of this meeting, the President left the Company and never returned. The owner chose not to investigate whether a kickback scheme was being perpetrated or any other possible wrongdoing. It was possible that because of the very close relationship with the materials suppliers, the President was authorizing above market value pricing to be charged to the Company with presumably some personal financial incentives paid by the suppliers. As the owner didn't wish to pursue the issue, we never were able to discover what may or may not have happened.

I had a client share a story very recently about copper being taken from a job site by one of his top field personnel who had been with him for over 20 years. This person took excess copper to a recycling business to sell it for scrap value. The owner of the recycling business suspected something wasn't right, asked the employee where they worked and was told the company's name. The owner knew the company and made a call to its owner from a back office phone while the senior field person waited at the front desk. The recycler asked the owner, our client, if he wanted the police called. Our client responded no, and to just send the employee back to the office. The senior field person was fired on the spot and word quickly spread throughout the company. Two days later another employee walked into the company President's office offering \$50. When the President asked what it was for, the employee responded that earlier in the week he had filled up a personal vehicle and later realized he had used the company gas card to do so. A culture of non-tolerance was created with the firing of the senior field person. If that field person was fired, anyone in that company was subject to being fired for any similar offense. It's hard to say whether that was the first time a company gas card was used for personal benefit, but we can all make guesses on that subject. An important point to note is the response by management and the creation of a culture of zero tolerance.

What Can You Do About It? Fraud is rampant and is a sad fact of life in our world. I'm not sure you can ever put a complete stop to all the ways that money, goods, or services for that matter can be stolen. That being said, there are many ways you can mitigate fraud and the chances that it will occur in your business. Here are just a few items to consider...

- Consider obtaining a bond on certain employees

The cost of a bond is possibly cheap insurance should embezzlement or other fraud occur. Also, if you let prospective employees know that you will be bonding them and as part of the bond application the bond company will conduct thorough background checks including criminal, etc. you may find that the candidate decides that another opportunity he/she has is better for them. With this practice, you may prevent a possible bad apple from preying upon your company in the future

- Perform Criminal and Credit Background Checks

Employees to whom you will entrust financial assets should be checked; perhaps even conducting a check on a receptionist who may open the mail and list out the checks -- we had one situation, where over 6 weeks an employee was stealing checks straight from the mail. Be sure to get the appropriate legal permissions to conduct these checks from the prospective employees. Asking for this permission could also have a similar effect as discussed above regarding the prospect deciding that perhaps they should try their luck with a different employer.

- Make these employees take at least two weeks of vacation per year

Do not let employees forego vacations and get paid out unused vacation or carry over unused vacation. The idea here is that most of the embezzlers work very hard to cover up their trail. If you take them out of that job for a few weeks a year, that trail will most likely surface and any wrongdoing will be uncovered.

- Look for changes in employees lifestyles, circumstances and/or behaviors

As noted in one example above, a change in a spouse's employment situation could be a catalyst. Look for a brand new luxury car in your company's parking lot that you might suspect could be outside the expected financial ability of your employee. In a few of the cases we're aware of right now, gambling addictions are a common thread. Authorities have traced a few of the Controllers to Southern California Casinos. There are many indicators, if one is alert, which could lead to the identification of fraudulent activity.

- Monitor your financial statements and management reports for unusual fluctuations

As discussed in one example above, we noticed a spike in the cost of materials relative to earned revenue. That

fluctuation in a simple metric alerted us to the possibility of a kickback scheme. Monitoring financial reports can provide clues as to the possibility of fraud occurring. When cash leaves the building, often times the general ledger will reflect that activity. Paying close attention to your company's financial metrics will allow you to understand what a "normal" range is and if the numbers stray outside the norm, it could potentially be an indicator of fraud.

- Prosecute and Communicate

As noted in one example above, the creation of a culture of zero tolerance is important. In another case discussed above, the owner was able to recover approximately \$60,000 almost immediately by letting the individual know that the authorities were going to be brought in. That individual thought that making partial restitution would prevent the prosecution process from occurring, but they were wrong. The situation was communicated to all the employees as it was happening. The owner was careful to stick to only the facts as he knew them. The underlying message was that this activity was not acceptable, would not be tolerated and would be prosecuted to the fullest extent of the law.

- Always have an invoice or other support attached to the back of any check you sign

Oftentimes due to the large volume of checks owners will sign, they only will handle the checks themselves and sign in short order, without taking the time to review supporting documentation to ensure the expenditure is justified. A Controller may run into the owner's office with only the check and ask for a signature. The payee may be familiar -- let's say "American Express." But is it the owner's American Express account or someone else's account? You don't know unless you have the backup for the check agreeing to the check amount. Take the time to review the backup, as it is a common sense practice that is worthwhile.

- Run a vendor history showing invoice numbers and amounts

You may find an interesting trend by simply running a vendor history. Would you agree that it would be peculiar if the history showed a sequential order of invoice numbers (e.g. 1001, 1002, 1003, 1004, etc.)? I would find that very odd as this would indicate you are the only customer of this vendor which is highly unlikely. This type of invoice number pattern could indicate a fictitious vendor was established by someone in your office.

- Conduct Seminars about Workplace Fraud

Creating an awareness in your business about fraud is important. Educating your employees about fraud, letting them know how prevalent it is, what the consequences are, and that it is not tolerated is a step towards prevention. Coordinate with your HR Department and your labor law attorney to ensure you are communicating the issue appropriately.

- Be sure to communicate the need to issue a 1099 to the embezzler

In Wikipedia's discussion on embezzlement there is discussion, based on case law, that the proceeds from the embezzlement are to be included in taxable income. This should be communicated to the person who embezzled funds and explained that if they make remuneration in the same year, then those amounts would not need to be included in taxable income. That could be one of the factors motivating an individual to make restitution.

- Provide instructions to your bank

In many of the cases I've seen over the years, the embezzler will write checks out of the operating account directly to him/herself. Instruct your bank to never honor a check from your operating account written to an individual. It is also a good policy to provide your bank with a list of your approved vendors to whom checks written may be honored. Of course you'll need to continuously update that list as you add vendors but that isn't as onerous as it may sound. Your Accounts Payable clerk will need to add a new vendor to your accounting system to write the check in the first place. Make communicating these vendor updates with your bank a part of that same process as setting up the new vendor in your accounting system.

Also, be sure to provide your bank with a list of your employees. Instruct the bank to only honor payroll checks written to names on that list. As with the new vendor procedure listed above, have your HR Manager or Controller regularly communicate new employee names to the bank to add to that list and delete names of those employees who are no longer associated with the company. Have a copy of the bank statements, or the originals, mailed to your home. Review each statement for appropriate employee and vendor names.

- Hand out employee pay checks at least once a year

Require each employee to provide identification when picking up their paycheck. The paychecks you may have left over will be for those employees who are on PTO (vacation, sick, etc.) that day or perhaps those "employees" who don't exist. These checks are for fictitious employees established by someone in your office. There are rules and regulations, certainly in the construction industry, regarding where you must hand out the checks. You may have to go to each job site to physically hand out the checks. In that case you may want to, on a monthly or quarterly basis, rotate which job sites you or your designee will visit.

- Participate in a limited scope fraud program

Your CPA firm may have a program in place to perform spot checks for unusual activity in certain areas of your business and therefore decrease the chances of it happening in the first place. After the first time or two that your Controller and other accounting personnel note that you are bringing in people to perform procedures specifically designed to help

lessen the chances your company will be victimized by fraud, the greater the chance that they themselves may not engage in that activity to begin with. There is an old saying “Employees do not do what we expect, they do what we inspect”. If you are inspecting for possible fraudulent activity, the chances of employees engaging in that practice should decrease.

Conclusion Fraud has been part of our society for thousands of years. It is driven in part by greed and sometimes by fear. Preventing it in absolute terms is most likely a losing proposition. Implementing controls like having an outside party come in periodically to perform procedures to help identify unusual activity, being alert to changes in your employees behavior and circumstances are all ways to help prevent fraud. Do not tolerate fraud if you experience it in your company…prosecute. If these criminals are not prosecuted, the chances of one of them landing in your company and doing the same to you is increased. Lastly, be aware that the chances of you becoming a victim are very real. This type of activity happens every day, everywhere. Position yourself by being proactive and be alert so that you lessen the chances it happens to you and your company. Glenn Carniello is a Certified Public Accountant and Certified Construction Industry Financial Professional. He is the Partner-in-Charge of the Orange County office of SingerLewak, Accountants & Consultants. Glenn has been in public accounting since his graduation from college in 1990. During his career, Glenn has provided accounting, auditing, tax, and consulting services to many of the firm’s construction, environmental consulting, manufacturing, distribution and nonprofit clients. He directs the Construction Industry Group at SingerLewak. He can be reached at: 949.261.8600 or gcarniello@singerlewak.com