DON'T LET SMALL LEAKS SINK YOUR SMALL BUSINESS!

The robber, we'll call him Mark, drove up to the bank and found a parking spot conveniently near the door. "Not busy for Noon on Tuesday", he thought. He took his note, placed his weapon in his pocket, and calmly walked into the bank. While this may seem like the start of a typical bank robbery, Mark was not there to rob the bank…he was there to rob his employer. His weapon was a ball-point pen and his note was a deposit slip.

Mark works as a Controller for a small distribution company and thus has responsibility for the company's financial processes. The company operates with limited staff and therefore lacks many of the internal controls that would be present in larger organizations. Mark had taken a check payable to his company and deposited it into an account that he had recently established with a name similar to his employer's. To cover the missing payment, Mark issued a credit memo for defective goods to clear the customer's account. Mark felt that he was underpaid and was envious of the owner's lifestyle. He justified his larceny as necessary to maintain his comfortable standard of living.

Across town the bookkeeper for a local construction company, we'll call her Mary, was preparing the payroll checks for the previous week. On her own timesheet she changed the one hour of overtime that she worked to nine hours. Also, over the last several months Mary had established a "ghost" employee in the payroll system and issued fraudulent checks that she would cash. Mary was a single mom struggling to meet expenses and promised herself that these were just "loans" that she would eventually repay.

In its *2018 Report to the Nation on Occupational Fraud & Abuse*, the Association of Certified Fraud Examiners estimates that U.S. organizations lose 5% of their annual revenues to fraud. The median loss to a small business with fewer than 100 employees was $200,000. Occupational fraud schemes often continue for years before they are discovered, and small

businesses are especially vulnerable as they often lack appropriate internal controls and proper management review.

The economic cost to a business that has fallen victim to fraud is troubling, especially in a difficult economic climate. A relatively small $10,000 fraud perpetrated on a small business that typically reports 5% net income will require the business to generate an additional $200,000 in sales revenue, just to cover the loss. It is not likely that the fraudster will stop there, however. Unless detected, the losses will continue to grow…often with devastating results.

The financial impact of fraud on a business goes far beyond the monetary value of the loss. The corresponding decreases to the bottom-line impacts (a) the working capital necessary for future growth, (b) bank funding criteria and the company's ability to repay debt, and (c) profitability calculations should the owners contemplate sale or merger.

While fraud cannot be prevented with absolute certainty, it can be deterred. Even businesses with relatively small staffs can implement a few practices that will greatly reduce the likelihood that they will be a victim. These are:

1. Tone at the top. It is not likely that the staff will strive for high ethical standards if the owners do not set a proper example in their dealings with customers, vendors, and employees. Management should establish an objective business climate where the employees perceive that the business values its reputation and demonstrates that on a daily basis.

2. Staffing. It may seem obvious that companies should not hire employees who have stolen previously but, unfortunately, that often does occur. At a minimum, references to prior employers should be contacted and drug tests and criminal background checks should be conducted to eliminate potential problems. Signed authorization from the candidate may be required so be sure to secure legal advice appropriate to your state.

3. Perception of Detection. Employees who perceive that they may be caught committing fraud will be less likely to attempt it. Employee training and related documents should include a section on ethics and the code of conduct for the business along with a statement of acceptance that each employee should sign. This is relatively inexpensive to implement and far cheaper than recovering from a potential loss.

4. Internal controls. Even a small business can take steps to lessen the possibility of fraud. Mandatory vacations, cross-training, and job rotation can almost always be initiated. The bank statements can be delivered to the owner's home if limited staffing requires that the same person who processes accounts payable also completes the bank reconciliation. Compare your operating results to industry standards and prepare ratio analysis and multi-year comparative financial statements to determine if your operating results trend out of norm.

5. Management oversight and communication. Almost half of fraud schemes are discovered by tips. Maintain an open-door policy and encourage employees to discuss their concerns. Take your staff to lunch occasionally and discuss the opportunities and challenges of the business and encourage their contribution. Know your vendors, encourage competitive bidding, review A/P check registers, pre-approve all payroll reports, establish budgets, identify variances, ask questions, and always read what you sign.

6. The outside accountants. Typical audit programs are not designed to specifically look for fraud and misappropriations and certainly do not test every transaction. Often, the outside accountants provide only a compilation of the company's financial reports and prepare the tax returns. An occasional, unscheduled, visit by your auditor or a Certified Fraud Examiner is a powerful deterrent to inappropriate activities. Any weakness in your internal controls may also be disclosed during this visit and appropriate corrective action will be recommended.

While small privately-owned businesses may be vulnerable due to the reasons outlined above, public corporations, government agencies, not-for-profit organizations and even religious organizations are often victims. The perpetrators will generally follow a common pattern of high motivation (excessive debt, gambling losses, perceived pay inequity, etc.), perceived opportunity (lack of proper authorizations and controls, no separation of duties, etc.), and rationalization ("borrowing" funds, "I'll pay it back later", etc.).

It is encouraging to note, however, that most employees are honest and truly committed to the success of the organization. Our workplace can be looked at as a mirror image of our communities. The vast majority of our citizens are law-abiding and work hard to provide a secure and comfortable environment for their families. Municipal funds budgeted to prosecute financial crimes deprive communities of benefits otherwise allocated to education, medical care, and the environment. The financial resources in any organization are similarly limited and losses due to theft negatively impact the ability of companies to provide salaries, benefits, and improvements to working conditions.

The current economic business climate can be viewed as a sea of uncertainty. Business owners are continually challenged by customer demands, price fluctuations for goods and services, government regulations, and their ability to attract and retain the best employees. Following the recommendations discussed in this article will help assure that ethical practices and controls have been adopted and the owners can appropriately focus their attention to steering their ship of state through this turbulent sea.

Don Dobesh, MBA, CFE

Mr. Dobesh is a Certified Fraud Examiner in Central Florida and has also taught forensic accounting and fraud examination as an adjunct instructor at the Keller Graduate School of Management.