

BLUE RIDGE BUSINESS JOURNAL

Serving Roanoke Valley/Lynchburg/New River Valley

VOL. 19, NO. 7, APRIL 9, 2007

bizjournal.com

Reprinted with Permission

COMPANY POLICY

How to avoid the gathering thieves at the office door

Fraud and its sometimes devastating results can spring upon your business before you know it, unless you are prepared. Here's how to prepare

Ahhh . . . Enron, World Com, Tyco . . . embezzlement, fraud, deception, greed. It all happens somewhere else. Or does it? A quick look at the local paper will show far too many incidents involving the deception of trusting organizations and businesses—treasurers for Scouts and fire departments, business bookkeepers, financial advisors, county supervisors, election and law enforcement officials. Trust is necessary in a business, but not to the point that you are “asleep behind the wheel.”

Investigators and auditors refer to something called the Fraud Triangle, three elements necessary for fraudulent activity to occur. Those three elements are motive, opportunity and rationalization. Motive and rationalization are elements belonging to the perpetrator; opportunity is often a door left wide open by an unaware business owner. Protect your business by regularly practicing certain procedures. Some of these include:

Open and review the bank statements every month. Do this every month before forwarding the statements to the accounting department. Since Check 21 went into effect, most of us only get photocopies of the fronts of cleared checks. It is still important to review the checks each month to identify irregularities. Look for any vendors whose name you don't recognize. Look closely at handwritten checks if most of yours are computer-generated. Review monies wired in and out. Does the cash balance look reasonable? Any of these items could alert you to things that may need further investigation.

Limit cash transactions. As much as possible, limit cash transactions. If that is not possible, increase the number of employees taking part in the transaction. If you have cash



Susan Culbertson
Columnist

register tapes, review when the sales are rung; a fourth of the day's sales being rung in the last fifteen minutes could indicate a bigger problem. Also, encourage customers to make payments to a central location. It doesn't make sense to allow a \$10/hour repairman to accept cash payments for a \$750 job.

Know your vendors. Identify the vendors that you use. If a check has been cut to a vendor you do not recognize, pull the original invoice. If you are still in doubt, call that vendor using the number in the phone book, not the one on the invoice. Phony vendors sometimes will not have a phonebook presence, but rather will have a prepaid cell phone account ringing into a backroom location with their other phony businesses.

Also, look up the vendor, using a conventional search engine. Put the street address (no suite number) in quotes with the zip code outside the quotes (e.g., “1600 Pennsylvania Ave” 20500). Look to see if other businesses are listed at the same address, especially if those businesses are UPS Stores (formerly Mail Boxes, Etc.). Often, fraudulent businesses lure customers with their fourth floor “suite” when what you really have is a business operating from BOX 410 at the local mailbox store. All businesses at UPS stores are not fraudulent; some businesses, however, lend themselves to a brick-and-mortar presence and an MBE box would not be appropriate.

Look at your business' listing of all vendors. Do any two vendors have the same addresses?

Compare the vendor list to the payroll list; are any of the vendor addresses the same as an employee's address?

Know your employees. Review the payroll list for possible fictitious employees. If you have a large number of employees, make an effort to meet a few new ones each month. This will spot check your list as well as create an open atmosphere for employees who want to report fraudulent activity.

The more you know about your employees, the better you will be able to determine if they are living beyond their means. Cars, homes, vaca-

tions, debt payoffs, large gifts to family and friends are all potential indicators if they exceed what you believe to be the family income. While the FBI reminds us that defendants are innocent until proven guilty, read their press release on the case in Massachusetts, where the embezzler allegedly started small and managed to steal \$6.9 million. Remember, the greatest opportunities lie with the employees who are most trusted or least paid.

Prepare and use a cash budget. In addition to your accrual budget, prepare a cash budget yearly. This is an excellent management tool, and it would help to identify cash fluctuations quickly. See the example of how the cash budget differs from the accrual budget.

Keep an eye on suspense accounts. This is especially true when the account is high-volume, but low-balance. These tend to fly under the radar. Some software packages won't even show monthly transactions on an account if the end of the month balance is zero. Limit the use of suspense accounts, if not eliminate them altogether.

Know insurance's limitations. While you may feel secure in the insurance you have purchased to cover fraudulent situations, discuss details with your agent or carrier. Often, the required time to report a claim is when you suspect that there will be one, not later when you are sure. Also, insurance will often not cover employees known to be fraudulent.

Whistleblower access. Provide several means by which employees can report suspected fraudulent activity. Often staff employees know of irregularities, but do not feel safe in reporting their suspicions for fear of reprisals should they be incorrect.

If all else fails, never fear: greed always trips up the perpetrator in the end. Don't wait until it gets that far. War-gaming possible ways to steal from your own business will keep you one step ahead of those actually trying to do it. To formulate ideas, look at FBI press releases to see how some of those frauds occurred and how that could be applied to your business. Establish your own monthly procedures. Close any open access to cash, inventory and other valuables in your business.

Remember, limit the opportunities and you limit the fraud.

(Susan M. Culbertson, a CPA, is with Controllers, Etc. in Roanoke. She's at www.controllersetc.com.)