STEWART G. LIEBLING, P.A.
CERTIFIED PUBLIC ACCOUNTANTS

July 20, 2009

Re: Creating Effective Internal Controls

Dear Clients et al:

Employee theft is extremely common. People steal office supplies in the fall (to use as school supplies for the children), deal with vendors who provide kickbacks (often in the form of expensive gifts and services), and sometimes even find clever ways to steal inventory and pilfer cash.

Most people don't steal, but embezzlement does happen; so it makes sense for you to consider what you can do to minimize your employees' opportunities to steal. Here are some great ideas you can use to reduce your chances of employee theft, and create effective internal controls.

Segregation of Duties

No single employee should control a financial transaction from beginning to end. The person who writes your checks should never be the person who signs your checks. The person who opens the mail should not also record the receivables and reconcile the accounts. The person who opens, reviews, and reconciles the bank statements should be different from the person who creates the deposits and checks within the company. By dividing up responsibilities, you will make it more difficult for a person to steal from you and manipulate your records to cover it up.

One of the most common ways to embezzle money from an employer is called lapping. To lap, an embezzler skims a little bit of the cash that comes in each month and then adjusts the books to hide the skimming. As long as the person skimming the cash also maintains the checkbook, its easy for the theft to go unnoticed. The embezzler simply ignores or hides the fact that, for example, the $500.00 Customer owes you has been paid.

You can minimize the opportunities for lapping by having one employee open the mail and make a list of the incoming cash and another employee enter the bank deposit information into the checkbook. For this approach to work, you simply compare the list of incoming cash maintained by the mailroom person with the bank deposit information shown in the checkbook, and you contact customers about past-due payments. This way, you can discover, for example, that Customer A actually paid the $500.00 owed and that their check has cleared the bank.

6705 Red Road, Suite 608, Coral Gables, FL 33143
Phone: 305-663-5313 Fax: 305-668-3089 Email: stewartl@sglpa.com
Website: www.sglpa.com

Get your bank statements personally

Don't give a person who is in a position to embezzle a chance to destroy or remove evidence of the wrongdoing. You should receive unopened bank statements and canceled checks each month. Review these checks carefully. Examine the payees, signatures and endorsements on each check. Keep an eye out for indications of fraud such as:

- Checks to suppliers or people you don't know
- Checks made out to cash that are larger than the amount you allow for petty cash
- Signatures that look forged
- Missing checks, or check numbers that are out of order
- Checks made out to a third party but endorsed by someone in your company
- Checks where the payee listed does not match the name in your register

Closely guard your company's checks

Don't be careless with your corporate checks. Keep them in a locked drawer and don't give out the key. Use pre-numbered checks, and check for missing check numbers frequently. Have a "voided check" procedure in place that requires you (the owner) to validate all voided items. Require all checks above a nominal amount to have two signatures (one of which is yours).

Sign every check personally

It's a good idea to sign all checks, even the small ones-yourself. This can be a lot of work, but you can have an employee prepare the checks for your review and signature. The benefit of signing all your checks is that your signature will be a requirement for money to leave the business. No cash will be deducted from the business bank account without your knowing about it.

Review the checks to make sure they are for people you know. If there's a name you don't recognize, go find that person. Keep a weekly count of the number of people on your payroll, and verify that number against the number of checks you have. Make sure that changes can not be made to your company's payroll master file without your approval and signature. Another option: have a separate bank account for payroll, and deposit the exact amount of your payroll in that account; then insist on a prompt monthly reconciliation.

If you sign all checks, an employee who wants to steal cash from you might try to convince you to write a check that the employee can cash. (You wouldn't write out, say, a $1,000 check to the employee without asking questions. This means that the employee would need to set up a fictitious vendor and then convince you to pay this vendor some amount. Or the employee might have you pay someone the employee needs to pay anyway. By carefully reviewing the checks that you sign, you minimize the employee's opportunities for committing these crimes.

If you'll be on vacation for, say, a couple of weeks, the business will probably need to pay someone while you're away. You can deal with this in a couple of ways. You can decide to trust an employee enough to leave behind a signed check or two; the employee can then use these signed checks to pay for things such as an unexpected C.O.D. shipment. Or you can decide to simply require vendors to wait. If you leave signed checks, be sure to leave specific instructions as to what these checks should be used for, and review the checks when they come back from the bank to be sure that your instructions were followed.

Prepare Timely Bank Reconciliations:

Bank reconciliations should balance and be performed timely. Periodic review of the checking account register by the owner (or controller), will deter thoughts of misdeeds. Statements that consistently do not reconcile may be an indication of employees helping themselves to company assets. Review bank statements very carefully, check for unfamiliar fees charged by third parties, and check bank statements online at least twice a month. Bank balance adjustments should require approval from an employee other than the individual(s) entering the transactions.

Consider having our office complete the bank reconciliation when you have too few employees to adequately segregate important financing activities. With a high speed internet connection, reconciling your account from our office is easily accomplished. The owner can participate by opening the bank statement envelope and reviewing the cleared transactions before anyone else. Keep an eye open for unusual electronic withdrawals, and compare deposits per bank to a deposit report within your accounting system for the same period.

Watch your receivables closely

Have more than one employee involved in counting and verifying incoming receipts. Make sure all incoming checks are properly endorsed. Consider buying a "for deposit only" stamp, and use it on all incoming checks - this can prevent an employee from cashing them. Personally investigate customer complaints that credit has not been received for payments. Get a copy of the front and back of the customer's check, and be sure it was deposited into your business account.

Require Vacations

There's a final embezzlement prevention tool that many big businesses use and that you should probably consider: Require regular vacations of a week or two. (Banks almost always do this.) Make sure every employee takes regular vacations. If fraud activity exists it is likely to be detected when someone else assumes the job temporarily. Here's the rationale: Some embezzlement schemes are so clever that they're almost impossible to catch. The one typical weakness of these super-clever schemes, however, is that they usually require ongoing maintenance on the part of the embezzling employee.

If fraud activity exists, it is likely to be detected when someone else assumes the job temporarily. Here’s the rationale; Some embezzlement schemes are so clever that they’re almost impossible to catch. The one typical weakness of these super-clear schemes, however, is that they usually require ongoing maintenance on the part of the embezzling employee.

Make sure you understand your books

Embezzlement commonly occurs when bookkeeping is sloppy and unsupervised, which makes it easy for an employee to keep cash and receipts.

As the business owner, you must be familiar with your company's bookkeeping and record keeping system. This way you can easily review the books and make sure nothing is amiss. If you're not a "number person," have us spend some time with you to show you what to look for, or take an accounting or bookkeeping class at your local college. Trusting someone else to oversee this most important part of your business only opens the door to fraud.

Secure your bookkeeping software

Don't allow unauthorized access to your bookkeeping software. Don't put the computer that holds your books on your network. Make sure both the computer and the software are password-protected. Change the password frequently to lock out unauthorized persons from this program.

Audit Trail tracks deletions/modifications to transactions.

Using the audit trail feature in some accounting software creates more data and larger files, but it is a great help in checking out who did what and when. QuickBooks users can turn on the audit trail from the Edit menu> choose Preference>click on Account in the left-hand scroll box>from the Company Preferences tab, select the "Use audit trail checkbox." click OK. The audit trail feature will keep a record of all transactions entered, every transaction revision, date/time of revision, and the individual's name. Audit trail reports are available under "accountant & taxes" menu option within the reports menu.

Protect Other Valuable Assets

From an embezzler's perspective, cash is the most convenient item to steal. It's portable, easy to store, and easy to convert to other things an embezzler might want. Because cash is usually watched so closely, however, embezzlers often steal other items of value, such as office equipment, inventory, and supplies.

You can follow a couple of general rules to minimize losses such as these. You can keep a record of the things that your business owns and periodically compare what your records show you have with what you actually hold.

If you buy and sell inventory, for example, keep a record of what you buy and sell. Then, once a month or once a year, compare what your records show with what you have in your warehouse or storeroom.

You can also restrict access to any valuable assets that the business owns. Warehouses and storerooms should be locked. Access should be limited to people who really need what is being kept behind lock and key. If you have items of high value in a storeroom, for example, and several employees have access, it's also a good idea to make it a rule that people go into the storeroom only in pairs. (A dishonest employee is less likely to steal if someone else is present who may see and report the theft.)

Pay Attention To Red Flags & Investigate Immediately

- New hires quit soon after starting
- Vendors who insist on dealing with just one individual
- Unable to identify the cause of lower gross margins or high overhead
- Employees with unreasonable close relationships with suppliers
- Customer complaints of missing invoices or transactions on invoices that were not ordered or received.

A few do's and don'ts to improve your internal controls:

- Former owners may not make for good employees
- Banks do not check the endorsement on each check you write, so make sure you make it a step in your monthly bank reconciliation. Look at checks made payable to unknown vendors or persons; checks made out in even amounts; dual endorsements; and checks to cash and to employees. (**Please note that we do not review or check endorsements when performing your monthly or quarterly bank reconciliations for you. Additionally, we do not review each check you write unless you specifically request us to do so in writing**).
- Segregate financial duties- approve payments, write checks, bank reconciliations, place orders, apply customer payments, etc.
- Have a complete written supporting documentation for each financial transaction. Do not allow accounting to rely on continuous verbal assurances from the employees who hold supervisory positions.
- Back up your accounting software file and keep the backup off premises away from the harm of a disgruntled employee. Think about using the remote access in the QuickBooks Premier version to easily transfer data files to safe offsite locations. (**Additionally, many of our clients send us a full backup version of their QuickBooks on a weekly or a monthly basis using www.yousendit.com**).

We would be happy to discuss this letter and assist you in implementing these suggestions. Please give us a call to setup a meeting to discuss this further.

Sincerely yours,

Stewart G. Liebling, CPA
Stewart G. Liebling, P.A.
Certified Public Accountants