PROTECT YOURSELF … FRAUD IS RISING!

With the booming economy and more people struggling to make ends meet, fraud is on the rise. It may surprise you to know that most fraudsters are first timers who happen upon a "Perfect Storm" of circumstances:

- Opportunity
- Need
- Rationalization

Some examples of fraud and embezzlement we have seen are:

- A bookkeeper suspected of questionable accounting quits and deletes the company accounting file and all back ups
- A bookkeeper inflates her gross wages and then increased her payroll deduction for federal income tax keeping her net wage about the same. She used Uncle Sam as her "piggy bank"
- Bookkeeper knew everyone's password on the system and would skim cash using different users to hide her tracks. She would also record checks written for payroll taxes in the accounting software but would handwrite the check to herself
- Manager would go back into cash invoices and remove parts from the invoice, placing them on another old open order to prevent an inventory issue pocketing the cash to the tune of approximately $125,000.00
- Manager would manage the collecting of the accounts receivable and would mark an invoice paid by cash to A/R and pocket the cash. He would also accept cash towards the customer's account and not record it adding up to approximately $80,000.00

The harsh realities are that when fraud occurs in a small business it averages almost $100,000.00 per year according to the Association of Certified Fraud Examiners. It takes an average of eighteen months to catch an employee and when you do, the cash is typically gone and very hard, if not impossible to recover.

According to forensic accounting specialist Victoria Marechal, fraud comes in many devious ways. Examples include misappropriation of cash, exaggerated expense reports; check tampering, inventory theft, skimming cash, payments to fictitious companies or persons, kickbacks, diverting credit card payments to name just a few methods.

So who can you trust? Embezzlers come in many guises. Often it is the people you least expect. The likely profile is a long-time employee, the person you could really count on to not miss a day of work, be on time and readily dismisses accrued vacation time. It could be someone overwhelmed by gambling debts, mired in medical bills, or just plain disgruntled; even a family member can take advantage of loose accounting procedures.

If you would like to tighten up your accounting procedures but don't know where to start, we have provided you with the Top Ten Tips to Prevent Fraud.

1. Send Bank and Credit Card Statements to a Separate Address. Do not send your bank statements to your business address. Have your bank statement sent to your home, PO Box, or lockbox address. Review each check both front and back for payee, signature, and endorsement. Even if you don't allow your employees to use your credit card, make sure those statements are sent to an alternative address too. Examine each statement carefully. Review each and every line item of both payments and charges.

2. Do Not Let Anyone Misrepresent Themselves as You. Do not let them use your password, sign your name, or use your credit card, ever. Never let an employee sign your name, use your credit card, or misrepresent themselves to your bank or Credit Card Company. Reimburse their expense. Don't reveal sensitive passwords. If you allow your employee to sign your name even on credit card purchases, it could compromise your legal recourse in case of fraud or embezzlement.

3. Reconcile Bank Accounts and Review Statements. Review every statement. Make sure all bank accounts and credit cards are reconciled. Afterwards, take time to review every reconciliation report. Notice stale checks or deposits that have not cleared the bank. Check for missing deposits. An increase in the number of reconciled items may also reveal mischief. **Side Note:** We find reconciling accounts to be a very productive exercise as we have found duplicate charges a number of times on bank and credit card statements.

4. Assign Administrative Rights Effectively. Use the Administrative rights in your management & financial software to protect your data. The first person to set up your software is typically by default assigned as Administrator. This role has unique permissions. So the administrator should be designated to either an outside party, i.e., a CPA or the savvy owner. Make sure that every user is set up separately and that passwords are used. Each password should be known only to that user. This protects the owner and others from liability. Make certain if an employee walks away from their computer they log out of the respective programs to keep someone with lower permissions from walking up to the computer and accessing areas they shouldn't. Lock down permissions to change or delete transactions. **Especially important:** Use passwords for closing dates.

5. Use any Audit Trail functionality in your software. It is wise to maintain a strict paper trail. Supporting documents need to be readily accessible in your files and then archived according to the type of document. Document Service Order and Purchase Order numbers on vendor invoices – make sure those numbers are recorded in your accounting software to complete the audit trail.

6. Use the Voided/Deleted Transaction Report. After you have turned on the Audit Trail, and made its review part of your routine, periodically review the **Voided/Deleted Transaction Report** to see which entries which have been modified.

7. Establish Accounting Controls. The principle of countervailing power is the fundamental reason to use checks and balances in accounting. Split the responsibilities between staff members or outside accounting professionals. **Warning Sign:** If only one person writes the checks and reconciles the account, there is no double check. Separate the duties. Consider another person to do reconciliations so it is done by a person other than the staffer generating the checks. Perhaps a Certified QuickBooks ProAdvisor® or CPA can provide these services.

8. Adhere to a Numerical Sequence. Use a numerical sequence for all transactions. Invoice, bills, and checks which are numbered fall in a logical and chronological order. The

reason: To identify missing documents. Look at the bank statement for large gaps. Secure paper checks. If you keep voided paper checks, remember to tear off the signature area to keep it from being misused. If your bank sends paper checks, sort them numerically.

9. Review Receivables and Payables. Look for adjustments to **Receivables** or **Payables**. Such adjustments could indicate subverted payments or vendor checks.

10. Back up Your Data. Repeat after me – Back up, back up, back up. Think redundant backups as a contingency plan for disasters of all sorts. Make scheduled copies. Rotate the media (tape drive or portable storage). If you use CDs, better buy the read-only variety. Store your backups at another location. Such diligence can come in especially handy if there is a disaster. In some fraud cases, the bookkeeper may delete all of the financial software files to avoid detection. In such cases the business has to pay a large sum for data retrieval, in hopes of capturing any shred of evidence. Be smart; back up. It only takes a few minutes.

If you have any questions or would like more information in creating checks and balances in your shop, just send an email to info@180biz.com or call (540) 833-2014 and we will be happy to assist you.

About Rick White & One Eighty Business Solutions

Rick White is a managing member of One Eighty Business Solutions (180BIZ), a Virginia based coaching and business solutions provider to the automotive and truck repair industries. Rick's clients consider him a trusted adviser, helping them to increase profits and free time while reducing stress. If you would like more business tips and thoughts just like this, please visit our Facebook page at www.facebook.com/180biz. 180BIZ provides affordable, down to earth, one-on-one business coaching with no long-term commitments. To see how we can help you and your business, please email us at info@180biz.com or call (540) 833-2014.