Beacon
SMALL BUSINESS SOLUTIONS, LLC

TRUST YOUR EMPLOYEES, BUT…

We have all read stories about some highly trusted and respected individual who has been charged with embezzlement of funds taken from a small family business or other organization.

Sometimes the person handles the funds for the local PTA, or sometimes it is the Treasurer for the local volunteer Rescue Squad, Fire Department, or other worthwhile organization we all would agree is a valued community resource.

And sometimes it is the Office Manager of your own company. Someone you have known for years and who has an emergency key to your house.

Never, ever is it anyone you would suspect. And yet, we'll see two or three stories each year. And with today's parlous economy, we just might see more than two or three before it's all over.

How do they do this? If your company or organization has multiple credit cards, and if the individual has access to all cards, they might rotate payments between cards.

Modern technology offers a variation on this theme. They scan the credit card statement, and, using readily available software, edit the statement down to a zero balance. The edited statement is then shown to the Owner, with a prideful comment: "See? I've paid us down completely!"

Another common strategy with multiple variations involves QuickBooks or other popular small business accounting software packages.

All these strategies center around the same theme: Invoice a client but divert the payment into their own account, and delete the invoice.

Or when receiving the payment, reduce the invoiced amount and pocket the difference.

Or deposit the check in the Bank, but use a Counter Deposit to get some of the money back. In this variation, the customer's Accounts Receivable is in order, it's the actual deposit that's the problem.

THERE IS NO SUBSTITUTE FOR OVERSIGHT BY THE OWNER. After all, it's the owner's money. And it's the owner's responsibilit

as published in YC magazine
York County's Entertainingly Informative Magazine

If we're talking about a community organization—and no, I don't have any specific organization in mind—responsibility often falls to the Board or other governing body.

Here are some simple things that can and should be done in all organizations.

First, don't let the person who prepares the deposit actually make the deposit. Do it yourself, or have someone else do it.

Separating the responsibility doesn't prevent the possibility of collusion between two individuals, but it sure makes it harder.

Same thing for credit cards. Many companies provide credit cards and/or gas cards to supervisors in the field. That's OK, but get someone else to reconcile the card.

Same thing for bank statements. Reconciling a business bank statement is an absolute must. For one thing, think about the lost sleep if you ever have the misfortune to undergo an IRS audit with accounting records that have never been reconciled.

One of my favorites is for the Owner to personally reconcile the bank statement if s/he has that skill, or to at least watch while the Office Manager does the reconciliation.

There are many stories in the forensic accounting literature describing how an abusive situation was first discovered by the Owner sitting in on the reconciliation.

Personally, I have never seen it happen, but I have talked to people who have. You know what they watch? Not the reconciliation on the computer screen. They watch the person doing the reconciliation.

The best safeguard you will ever have is having your employees know that you know, and that you are watching.

Here are some other ideas.

Make the deposits yourself, and compare the checks being deposited to the deposit ticket.

Do the same thing with the daily reports from the Merchant

1171 Market Street, Suite 206, Fort Mill, SC 29708
Phone 803 802 7676
www.beaconsmallbiz.com

Processing Report if you accept a large volume of credit cards.

Modern technology is a wonderful productivity aid. QuickBooks and its competitors, document scanners, PDA's, and of course online banking have transformed our small businesses.

Here's what one respected accountant recently said about online banking: "employees should never have access to online accounts…no online access at all…not at all means not at all."

He goes on to say, "Most courts interpret the Uniform Commercial Codes to allow 30 or even 90 days for an account holder to ID and report fraud. Most online banking agreements shorten that time dramatically so the account holder eats the loss…"

I won't go that far—online banking has become an essential, standard tool, and to restrict access doesn't make sense to me.

But I will argue that not taking sensible, easily implemented precautions regarding cash flow is an essential obligation of the Owner.

After all, it's the Owner's money