

Fraud Continues to Impede Construction Companies, 3 “Hot” Frauds to Watch For

So what types of fraud are hot right now? Three in particular to watch for are:

1. Scrap metal scams. Scrap metal is a valuable commodity, especially during periods of economic uncertainty. You may keep a close watch on what leaves your job sites, but do you watch what comes in?

Acting in collusion with an accomplice in the scrap or junkyard business, an unscrupulous employee can order more metal (copper is particularly in demand) than you need, hide the cost in job reports and sell the excess to the accomplice for cash.

To prevent this type of fraud, make sure no one person is responsible for both ordering materials and approving their costs. Additionally, someone other than the person who orders materials should check them in when they arrive at job sites.

2. Misbegotten mechanics. Another fraud that requires collaborative effort is that of false equipment repairs. In this scam, an outside mechanic submits phony maintenance and repair invoices. An employee then approves them and splits the resultant payment with the mechanic.

Again, oversight is the key to preventing such schemes. Someone other than the employee who approves maintenance costs should review invoices. If a cost seems off-base, the reviewer should check with equipment operators to see when — or whether — the work was done.

3. “Dead” vendors. In this scam, someone sends you invoices bearing the logo and letterhead of a company that’s closing because the owner has very recently died or retired or the company is no longer operating. Before you’re aware the company is “dead,” you’ve paid the bogus charges and the fraudster is off to another scam.

To prevent this one, pay close attention to the invoices that come in, and make sure you’re paying for something you actually ordered.

In addition to these frauds, construction companies are subject to the same billing, payroll, vendor and customer frauds that all businesses must guard against. To protect yourself, be proactive.

Establish internal controls that make it difficult for fraudsters to succeed, and adopt a “zero-tolerance” policy toward any type of unethical behavior.

Tips from employees and business associates outside the company are the most common way frauds are discovered. Make sure all workers know their responsibility in reporting suspicious behavior. Fraud is here to stay, but there’s no need for you to make it anything other than an unwelcome guest.

Payee Positive Pay

If you’re one of our many customers who have adopted payee positive pay to protect your company from check fraud, congratulations! Payee Positive pay has become the number 1 defense against check fraud in the United States according to the Government Finance Officers Association ¹.

Wright Office Solutions, Inc and JustinTime Software creators of JustinTime Payee Positive Pay will automatically create the file from Sage Master Builder to submit to your bank. Your bank will compare the payee name, check number and amount from the file submitted before cashing the check.

If your company is not using some form of payee positive pay, you’re exposing your business unnecessarily. Payee Positive Pay has proven its value in foiling attempted check fraud.

¹ www.gfoa.org/downloads/bankaccountfraudcash.pdf

For more information on JustinTime Payee Positive Pay contact us at sales@wrightoffice.com

Tech Support

Calls From Our Customers



Some of my cash transactions do not show up when I am doing my bank reconciliation.

We get this call often. Nearly every time it is due to cash transfers from one cash account to another. In SMB you must use a interim cash account for bank transfers. For example, you move money from a savings account to a checking account. You will go to 1-1 Checks and Bank charges. The account in the header will be the Savings account and the account in the grid will be a Cash Transfer or holding account. Then you will go to menu 1-2 Deposits and Interest. In the account field in the header enter your Checking account and the account in the grid will be the Cash Transfer account. This will give you a transaction to be cleared for each bank reconciliation and zero out the Cash Transfer account.

I need to close the month and SMB says I cannot log in as exclusive. I have checked all of our workstations and no one is logged in SMB.

Sometimes when a user is dumped from SMB their license is not released. There is a utility that is installed with SMB for just this purpose. Go to Start, Programs, Sage Master Builder, Sage License Administration Tool. Change Username to Other (View Only) and click Ok and Ok again. The tool will then open. Click on the line that reflects “Floating use” under the License Type heading. In the lower right box you will now see a list of who is logged in. You will need to end the task for that user at their workstation.