

10 Ways to Reduce the Risk of Fraud: Best Practices for SMB Internal Controls

7 min read



Key Takeaways

- Business owners and CEOs can take proper precautions to lower the risk of fraud such as a quick end-of-week review of the bank statement, automating bill payments, and making sure your files are secure.
- Many small business owners are looking for fraud prevention strategies that won't break the bank. For businesses using QuickBooks®, there are several built-in functions that can do this for you, but you have to take the time to set it up right.
- Whether you have separation of duties or if your accounting is outsourced, automating your billing, not only reduces fraud but also saves time and money.

No system of internal controls should be built on trust. For anything you don't outsource, adhere to the separation of duties and follow best practices for internal controls.

10 best practices to help reduce your business's risk for small business fraud:

1. Open & review the bank statement yourself

An obvious but critical task for reducing fraud is reviewing the bank statement. It's important that you do a quick scan and take notice of anything out of the ordinary. The bank statement should be received unopened — then scanned for any red flags, each check reviewed for authorized payee and signature, and electronic payments approved — before handing off to the bookkeeper.

We recommend an end of week quick review of the bank statement (depending on whether your business has a lot of transactions) with a monthly detailed review of the bank reconciliation.

According to [Investopedia](#): Small business owners should go through the bank reconciliation process at least monthly, and many business consultants recommend doing bank reconciliations weekly or even daily.

2. Don't let your bookkeeper reconcile the bank account

The person who pays the bills should never reconcile the bank account. That's how they cover their tracks. Detection of embezzlement is difficult when your bookkeeper is the culprit, as they have the knowledge and ability to manipulate your financial records and books.

Business bank accounts are not as protected as consumer accounts under federal law, which means you can't count on the bank to cover fraud and errors in your account. A drained business account can be devastating. - [The Balance](#)

3. Be Systematic in Accounting System Setup

Many small business owners are looking for fraud prevention strategies that won't break the bank. For businesses using QuickBooks®, there are several built-in functions that can do this for you, but you have to take the time to set it up right.

Every defined limitation provides another obstacle to theft. However, too frequently, the set up process is rushed and these critical safeguards are overlooked. You should never default everyone to full administrator rights, share logins and passwords, or give accounts to employees who really have no need for one.

[--> Signs Your Bookkeeper is Stealing and How to Prevent Fraud](#)

4. Separate opening the mail from the accounting function

The person who opens the mail, shouldn't be the same person who is responsible for accounting functions.

The person who opens the mail keeps track of any checks received

The person who opens the mail should keep track of checks in a physical paper log of what checks were received and when. The checks should be handed over to the bookkeeper or accountant with a copy of the list. This covers both the person who opened the mail, and the bookkeeper or accountant.

Be sure all checks are deposited daily to avoid potential for issues.

5. Don't let the person who does billing make the deposits.

The person who does the billing should not also be the person who deposits checks. Someone who does both can endorse a check to themselves and delete the original invoice.

You can avoid this form of fraud by separating duties so the person who does the billing is not the same person who is making deposits. By outsourcing the bookkeeping and controller aspects of the business, you are more likely to deter fraudulent activity since there's more than one pair of eyes watching your books.

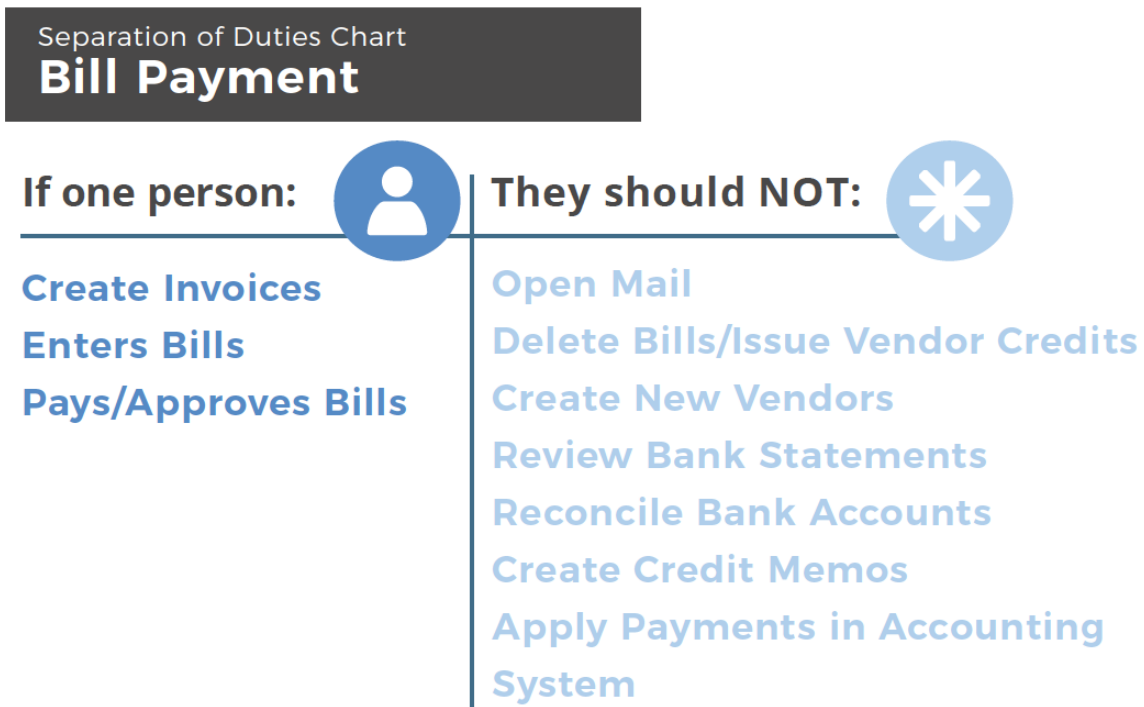
[Billing Fraud](#) - The most frequently occurring type of fraud in small businesses is billing fraud, which amounts to 27.1 percent of all cases.

6. Automate Bill Payment to Reduce Billing Fraud

Whether you have separation of duties or if your accounting is outsourced, automating your billing, not only reduces fraud, but also saves time and money. Manual bill payment can be costly, time-consuming and an opportunity for errors or fraud. Use a Bill payment app like Bill.com to automate processes.

A popular form of billing fraud is when an employee submits personal, padded, or completely fake invoices for goods or services to the employer. Some employees will even go so far as to submit invoices from fictitious companies they have created. Another tactic is to submit bills for personal items the employee purchased to write off as a business expense.

If one person creates invoices, they should not also apply payments in the accounting system.



7. Secure your files

If you must use your own bank's bill payment, use SmartVault® to link scanned images of every transaction to the QuickBooks file. You'll then know exactly what's getting paid, further protecting your files and reducing the chance for fraud.

Once the details of a source document have been entered into the accounting system, the document should be securely filed away in a place where it can be retrieved at a later date. Not only is it important to securely store the document, it is also essential that security and controls be placed on that source information, ensuring integrity by not allowing it to be moved, removed, or changed. - [SmartVault](#)

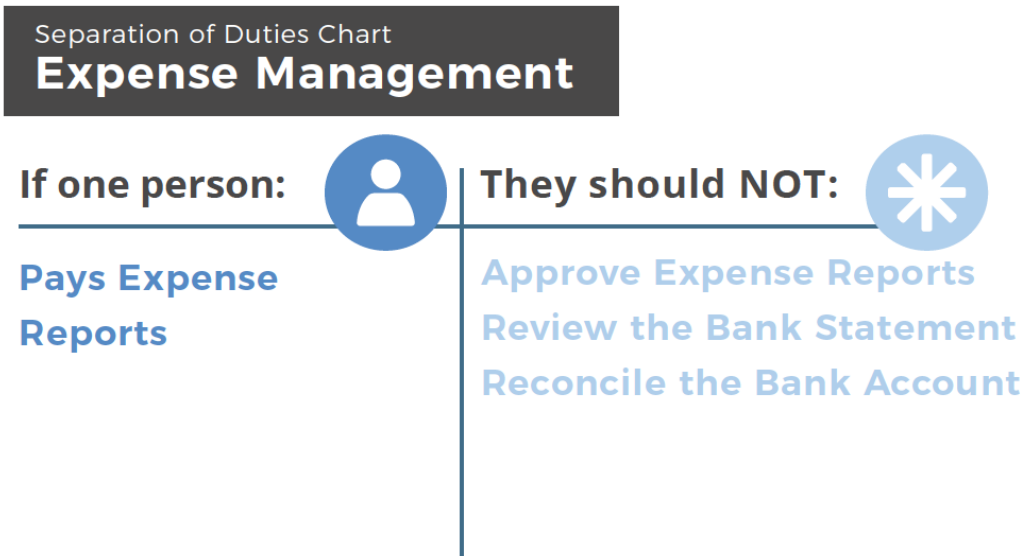
8. Automate Expense Management to reduce Expense Fraud

Expense reimbursement fraud makes up about 15 percent of business fraud with a median annual loss of \$26,000, according to [a study by the Association of Certified Fraud Examiners](#). And, according to this study, it takes about 24 months before expense reporting fraud is detected.

[--> 6 Signs Your Employees Are Abusing Expense Reports](#)

If there are no internal controls in place, a bookkeeper can submit reimbursable expenses and issue payments to themselves from the organization's bank account - reimbursing

themselves for personal expenses.



To reduce the risk of fraud with expenses, use an app like Expensify® or InSperty® Expensable, which require scanned images to be attached to reduce fake expenses being entered. Receipts must be submitted or any other kinds of proof to substantiate any reimbursement requests.

“Imagine automation that has the ability to memorize your company’s unique expense management policies and automatically determine which expenses actually need a manager’s review and which can get automatic approval.” - [Expensify](#)

9. If Your Bookkeeper Insists On Doing Payroll In-house - Ask Yourself Why

The cost of payroll services is low compared to the peace of mind gained from requiring your signature on any payroll change. A sneaky bookkeeper can do many things you can never see, if they also file the payroll tax returns.

Payroll fraud requires extra scrutiny

While payroll fraud only accounts for 8.5 percent of cases, the median loss per case amounts to \$90,000.[10] Because the amounts are so great, payroll fraud warrants special

attention. Again, the fact that small businesses typically lack internal controls makes them an easy target.

[Payroll tax fraud is one example.](#) Payroll tax withholdings are the amount an employer withholds and remits to the IRS on behalf of each employee, and that amount differs per employee, it isn't difficult for someone to conceal the additional funds and then intercept the mail to hide tax letters.

You should not handle payroll in-house. The risk is great and the cost to outsource it is very low. A best practice for preventing this type of fraud is to outsource this function and have a system of review to reduce the likelihood of false compensation claims.

10. Have an Accounting Policy Manual

Building a system of internal controls

Control activities are the policies and procedures that ensure management directives are carried out. They usually involve two elements:

- A policy that prescribes what should be done
- The procedure to implement the policy

Have a policies and procedures document in place that list all the requirements and expectations of employees. Have employees sign off, acknowledging their understanding of what is expected of them within your organization.

Fraud Prevention Checklist for Your Small Business:

- Does management set the right tone by setting the right example and enforcing a zero-tolerance policy?
- Do your employees understand what constitutes fraud? Is it clearly defined in the employee manual?
- Do employees believe they can speak freely when they suspect fraud is being committed?
- Do they know where to go for advice? Do you have a way for employees to report potential fraud?

- Are performance goals realistically attainable for your employees?
- Are anonymous surveys conducted to assess morale?
- Has a system of internal controls been put in place?

GrowthForce Applies the Team & Technology Approach

Our disciplined procedures mean fraudsters have nowhere to hide their crime, delivering great protection and peace of mind to the business owner. By working in teams with multiple layers of oversight, GrowthForce helps protect against human error as well as fraudulent activities. We also heavily screen each employee, and as added protection, carry insurance coverage for professional liability and employee dishonesty.

Your GrowthForce service team will compare and analyze each canceled check, review audit trail reports, lock down prior periods and ensure several sets of eyes are watching your accounts for any warning signs of employee theft and fraud.