PERSPECTIVES

FIVE FRAUD PREVENTION TACTICS FOR SMALL ACCOUNTING DEPARTMENTS

JS|HELD

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

Copyright © 2025 J.S. Held LLC, All rights reserved.

Introduction

Business owners are often stretched thin as they balance growing revenue with managing operations. This can be exacerbated in a small business environment where resources are limited. According to the Association of Certified Fraud Examiners' Occupational Fraud 2024: Report to the Nations (Report to the Nations), approximately 43% of fraud is committed in organizations with fewer than 1,000 employees. Large organizations have the resources to implement robust anti-fraud programs, as well as enough employees for effective segregation of duties.

According to the Report to the Nations, while fraud cases were relatively evenly distributed across organizations of different sizes, the second-largest loss among organizational size categories was in businesses with fewer than 100 employees, followed closely by organizations with 100 to 999 employees. "Because small organizations tend to have smaller budgets and revenue, such a loss can impact these organizations more acutely compared to larger organizations."[1]

But regardless of revenue size, how do organizations *without* enough employees for effective separation of duties build the necessary internal controls and processes to protect against fraud and ensure compliance with regulations? Whether a sole proprietor with a handful of employees or a mid-sized business with a small accounting department there are steps business owners can take to protect against fraud. This article examines five practical steps business owners in smaller organizations can take to build fraud-resistant operations, even without a full-time controller.

1. Resist the Temptation to Comingle Funds

This is a common pitfall that easily leads to inaccurate financial reporting and issues with regulatory agencies, and other third parties. Consider these examples:

» A business owner collects cash proceeds from daily sales and deposits a portion of the proceeds into a personal account and a portion into the business account.
» A business owner who owns several businesses uses funds from one business to pay expenses for another business.
» A business owner uses his or her personal credit card to pay for business expenses and then uses company funds to pay for the entire credit card bill, including personal expenses.

Particularly with closely held businesses, where the profit of the company typically translates to income for the owners, business owners sometimes use business and personal funds interchangeably. This is invariably a mistake. While it is true that business owners ultimately have a right to take advantage of the profits from their companies, ensuring transparency with clear separation between personal and business use of funds is critical.

In each of the examples above a lack of clear delineation between personal and business transactions can lead to improper revenue recognition, inaccurate expense reporting, and a risk to Corporate Veil integrity.[2] These issues in turn lead to operational and regulatory challenges, such as difficulties to properly value the business when seeking third-party financing or when trying to sell or divest a

[1] Report to the Nations, pg. 32.
[2] Corporate Veil protection is a hallmark of limited liability companies, limited liability partnerships, and corporations to protect the owners' personal property against litigation. Comingling of funds can blur the lines between personal and business assets making personal property vulnerable to litigation. Legal Disclaimer: This article is provided for general informational purposes only and does not constitute legal advice. The content herein is not intended to create, and receipt of it does not constitute, an attorney-client relationship. Readers should not act upon any information contained in this article without first seeking appropriate legal counsel from a qualified attorney licensed in their jurisdiction. If you have any questions regarding the matters discussed, please consult with legal counsel of your own choosing.

part of the business. Additionally, comingling funds can raise red flags with the Internal Revenue Service, leading to possible fines or penalties for inaccurate filings and partnership disputes if the comingling of funds leads to incorrect distributions.

Accurate financial reporting starts with proper delineation between business and personal use of funds. Businesses should have designated operating bank accounts and owners and executives should be issued corporate credit cards with a clearly defined process for expense reimbursement to prevent inadvertently or fraudulently classifying personal purchases as business expenses.

These steps will go a long way to ensure financial statements and key performance indicators (KPIs) are properly captured, which leads to the next recommendation.

2. Prepare Monthly or Quarterly Financial Statements and a Key Performance Indicators Dashboard

Ensuring a clear separation between personal and business use of funds is the cornerstone of producing accurate financial statements and gives business owners a correct and clear view of the business's financial performance. While a full-time controller is ideal to create accurate financial statements, it is not always feasible depending on the size of the business. In such cases, hiring an external CPA firm provides the needed expertise.

In the examples described in the previous section, a professional with a strong accounting background, such as a CPA, can help business owners navigate through the proper way to account for business revenue and expenses, and can advise on the appropriate way to distribute funds to the owners. Again, business owners generally have the right to distribute profits derived from a business at their discretion, but transparency in reporting is essential.

A controller or external CPA can help design business processes to properly capture financial activity, can ensure financial statements are properly stated, and can highlight trends over time. Additionally, a CPA can create a dashboard of three to five KPIs that business owners can use to measure progress toward strategic goals, monitor operational performance, and support decision making. Traditional KPIs include revenue growth, gross and net profit margins, average accounts receivable collection period, inventory stockout rate, customer growth, among many others. What is important to keep in mind is that KPIs should be tailored to the specific goals of each organization. Even when a business is profitable and generating sufficient cash flow, it can be easy to miss areas of concern brewing below the surface.

3. Divide Financial Duties and Approve Vendors to Reduce Risk

Segregation of duties involves breaking up business tasks into four functions: authorization, custody, record-keeping and reconciliation. It is designed to provide a higher probability that mistakes, or fraud will be caught by another person involved in the process. Below are examples of proper segregation of duties in two critical business processes, accounts receivable and accounts payable.

Accounts Receivable		
Function	**Role**	**Responsibilities**
Authorization	Credit Manager	Approve new customer accounts and authorize write-offs
Custody	Mail Room Clerk	Handle incoming payments and prepare bank deposits
Record Keeping	Accounting Clerk	Issue invoices, post customer payments and maintain customer balances
Reconciliation	Accounting Supervisor	Reconcile accounts receivable subledger to general ledger and investigate discrepancies

Accounts Payable		
Function	**Role**	**Responsibilities**
Authorization	Purchasing Manager	Approve new vendors
Custody	Treasurer or Cash Disbursement Clerk	Handle outgoing payment and sign checks or initiate electronic payment
Record Keeping	Accounting Clerk	Record approved vendor invoices in the accounts payable system and maintain vendor records
Reconciliation	Accounting Supervisor	Reconcile accounts payable subledger to general ledger, review invoice approval and verify payment logs

Segregation of duties is one of the most effective ways to combat against fraud. However, this level of separation is not always feasible in small businesses, which can make them more susceptible than larger organizations to billing, check and payment tampering, and theft of customers' payments schemes.[3] Billing schemes often involve employees submitting fraudulent invoices for fictitious goods or services that are then paid by the company via the normal payment processes. Detecting employee fraud is critical. These types of losses can include theft, embezzlement, computer fraud, forgery and more.

Consider these examples:

» An employee forms a shell company and opens a bank account using the new company name. The employee then bills his or her employer for fictitious goods or services under the guise of the shell company, issues payment, and deposits the payment into the shell company's bank account to which he or she has access.

» An employee prepares a check for a small dollar value to a commonly used vendor and obtains the owner's signature. The employee then alters the check by changing the name and amount but records the expense with the vendor name in the general ledger to avoid suspicion.

» An employee intercepts a check received in the mail for accounts receivable payment. The employee steals the check and writes off the receivable as uncollectible.

There are steps that organizations with a small accounting department can take to mitigate a lack of segregation of duties. Certain functions can be assigned to employees in other areas of the organizations. For example, a receptionist or office manager can be assigned to obtain vendor invoice approval from budget owners to combat payment to fictitious vendors. Fictitious vendors being created in the system constitute a significant risk. If the accounting department consists of only one employee, access to the creation of vendors in the system should be limited to the owner.[4]

Also, to maintain the integrity of checks, once signed, checks should remain in the possession of the individual with check-signing authorization (more on that in the next section). A receptionist or office manager can also be assigned to receive and open mail, promptly endorsing checks from customers and preparing bank deposits to combat theft of customer payments. To protect against employee interception of customer payments, business

[3] Report to the Nations, pg. 34.
[4] For companies that processes payroll internally, creation and deletion of employees in the system should also be highly restricted.

owners can sign up for the United States Postal Service's Informed Delivery service, which shows preview images of incoming mail.[5]

Regardless of the number of employees in the accounting department, business owners can leverage their accounting software's internal control features surrounding access. Additionally, each employee should have his or her own login credentials with limited access based on function. Only one or two individuals should have access to the Administrator function, ideally the owner and someone outside of the accounting department. Administrative access should be highly scrutinized. Allowing one individual to have "the keys to the kingdom" in terms of access, leaves an organization highly susceptible to fraud.

4. Monitor Bank Activity to Detect Payment Fraud

Ideally, the following activities surrounding cash should be segregated: payment approvals (for example, invoice payments or expense reimbursements), check preparation including bookkeeping, check signing, and bank reconciliation.

If full segregation of duties is not possible due to personnel constraints, two simple, yet effective controls to implement include:

» Restricting check-signing authorization (or online payment authorization) to one individual – preferably the owner.
» Business owners review of monthly bank statements and bank reconciliations, including copies of cancelled checks.

According to the Report to the Nations, organizations with fewer than 100 employees experienced check and payment tampering fraud 23% of the time, compared to organizations with more than 100 employees which experience this type of fraud 9% of the time.[6] Coupled with the fact that check and payment tampering fraud schemes typically go undiscovered for approximately 18 months,[7] active vigilance is imperative.

A common fraud scheme is for employees to write checks to themselves, or a fictitious vendor or accomplice and then change the payee's name to a legitimate vendor in the accounting software to avoid suspicion. Spending a few minutes per month reviewing bank activity can be an effective deterrent against fraud and can help identify anomalies early.

5. Perform Inventory Counts and Scrutinize Write-offs

For businesses that carry inventory, periodic counts are indispensable.

Consider these examples:

» A warehouse employee steals inventory and increases the inventory when performing a physical inventory count.
» A retail employee steals inventory and does not attempt to conceal the theft.
» A warehouse employee steals inventory and writes it off in the system as damaged.

For businesses that have software that tracks inventory, physical inventory counts allow businesses to identify discrepancies between

[5] Informed Delivery - Mail & Package Notifications | USPS.
[6] Report to the Nations, pg. 34.
[7] Report to the Nations, pg. 16.

system counts and actual counts, which can point to theft. In the first example, the perpetrator attempts to hide the theft by changing the inventory counts. An added layer of control against employees trying to cover theft is for physical inventory counts to be conducted by personnel who do not have custody of the inventory or by pairing employees so they can verify each other's counts.

The second example can happen whether businesses have inventory software or not. In businesses that have inventory software, theft will be reflected by discrepancies between system counts and actual counts. In businesses that do not have inventory software, theft will be reflected in reduced margins. For example, after performing a physical inventory count, a business that consistently marks up its inventory by 40% calculates an actual profit margin of 36%. This scenario points to the possibility of theft.

In the third example, the perpetrator has taken steps to conceal the theft by writing off the inventory. For businesses without sufficient personnel to ensure proper segregation of duties, only the owner should have the ability to write off inventory in the system. If this is not a feasible option, then business owners should scrutinize write-offs to identify patterns that may point to theft.

Inventory counts are essential to identify theft early but also act as a deterrent for future theft.

Develop and Perform a Fraud Risk Assessment Framework

In addition to the ongoing controls and monitoring discussed in this article, all organizations, regardless of size, should perform periodic fraud risk assessments. Fraud risk assessments provide methodical quantitative and qualitative measurements of the organization's risk for fraud. A CPA or Certified Fraud Examiner (CFE), whether internal or external to the organization, can help business owners develop a risk assessment that considers the specific needs and culture of the organization. The risk assessment should identify inherent risks based on industry, assess the likelihood of fraud occurrence by department, evaluate whether existing controls are working properly, and provide strategies for mitigating risk.

Most importantly, once a framework for a fraud assessment has been developed, it should be revisited periodically as changes in the business occur, such as the addition of new business processes, staff turnover, or changes in the economic environment.

Conclusion

Balancing revenue growth and operations is a challenge for business owners, particularly when resources are limited. But the risk of fraud and financial loss is real. Business owners can establish simple, but effective routines to help protect against fraud:

1. Maintain clear separation of bank accounts and credit card use to facilitate proper accounting and regulatory reporting.
2. Prepare financial statements, analyze trends, and review key performance indicators.
3. Segregate duties as much as possible, but at minimum:
   - » Personally open mail, endorse checks, and make deposits or delegate to someone outside the accounting department.
   - » Personally enter vendors and employees into the accounting system or delegate to someone outside the accounting department.
   - » Personally sign checks.

4. Review monthly bank statements and copies of cancelled checks to identify instances of check tampering or vendor fraud.
5. Perform periodic inventory counts to identify potential theft and protect profit margin.

These steps provide high visibility to areas of potential fraud. However, there are many other controls that owners of closely held businesses can institute to protect against fraud. A CPA or CFE can help business owners identify what makes the most sense for a specific business.

A CPA or CFE can also provide a risk assessment and can help design controls to mitigate against segregation of duties limitations. If fraud is suspected or discovered, a forensic accountant can help sift through financial records to pinpoint the areas of fraud and help business owners stop and prevent fraud.

Acknowledgments

We would like to thank our colleague, Pamela Hefner, CPA, CFE, for providing insight and expertise that greatly assisted this research.

Pamela Hefner is a Vice President in J.S. Held's Economic Damages and Valuations practice. She specializes in litigation consulting, utilizing financial analysis to provide business, financial, and accounting advice to attorneys and their clients throughout the commercial litigation and investigation process. As a certified public accountant (CPA) and certified fraud examiner (CFE), she has provided expert support across multiple industries, including retail, manufacturing, food and beverage, and local government. Pamela provides expert witness and consulting services in accounting, investigations, and litigation, with specific expertise in damages calculations, class certifications, and fraud examinations.

Pamela can be reached at pamela.hefner@jsheld.com or +1 229 337 4067.

This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal, or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation, or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.

J.S. Held, its affiliates and subsidiaries are not certified public accounting firm(s) and do not provide audit, attest, or any other public accounting services. J.S. Held is not a law firm and does not provide legal advice. Securities offered through PM Securities, LLC, d/b/a Phoenix IB or Ocean Tomo Investments, a part of J.S. Held, member FINRA/SIPC. All rights reserved.