Protecting Small Businesses from Fraud

Simple Controls Can Reduce Opportunities

By Linda A. Kapp and Gordon Heslop

According to the 2010 Report to the Nations on Occupational Fraud and Abuse, "Small organizations are disproportionately victimized by occupational fraud. These organizations are typically lacking in anti-fraud controls compared to their larger counterparts, which makes them particularly vulnerable to fraud." (Association of Certified Fraud Examiners [ACFE], July 2010, www.acfe.com/rttn/rttn-2010.pdf) Antifraud or internal controls provide necessary checks and balances to help businesses prevent or detect fraud and safeguard assets. Internal controls are important for businesses of all sizes, but they tend to be less prevalent in small, private businesses that have few employees. There are many internal controls that a small business can—and should—implement to deter fraud, even with staffing constraints. Having proper internal controls in place also helps businesses conduct operations more efficiently and effectively.

Before discussing specific internal controls, it is helpful to examine the factors that might lead an employee to commit fraud against an employer. While the title for the employee varies from business to business, this article will refer to the office manager as the one individual primarily responsible for handling the majority of financial responsibilities in a small private business.

The Fraud Triangle and the Fraud Diamond

The fraud triangle reveals three necessary mechanisms—perceived pressure, opportunity, and rationalization—that typically must exist simultaneously for fraud to occur. The fraud diamond enhances the fraud triangle by including a fourth mechanism, capability. Understanding the fraud triangle and the fraud diamond will help small-business owners understand why it is important to be more involved in providing oversight of the accounting processes in the business and why internal controls should be implemented.

Perceived pressure. This first component is represented by some need for money, whether an actual need or just a desire for more funds. Perceived pressure serves to provide an incentive for a potential fraudster to commit fraud. Perhaps the employee has a debt that cannot be paid, has a medical emergency, desires items outside of his financial comfort zone, or has some other pressure causing him to at least temporarily believe he needs or desires additional money. When the employee does not have a legitimate way to raise the additional funds, he might turn to stealing from his employer as an alternative.

Opportunity. This second aspect of the fraud triangle is simply the ability to commit fraud with little or no perceived likelihood of being caught. It is enhanced by a lack of internal controls when an employee has access to cash or noncash assets of the business and has little fear of detection. Good internal controls and owner oversight can best reduce an employee's opportunity to commit fraud.

Rationalization. This final component of the fraud triangle is represented by employees justifying, at least to themselves, why they carry out fraud against an employer. Perhaps they begin by only "borrowing" the funds with the initial intent to repay. They may continue the theft either because they need or want additional funds, or because it was easy enough to get the original funds, making it tempting to continue "borrowing." Other forms of rationalization are where the employee feels entitled to stolen funds or goods because she does not feel fully appreciated, feels she is underpaid, or just believes the employer can afford it.

Capability. The fourth component, expanding on the fraud triangle and included in the fraud diamond, is capability. It is defined as "personal traits and abilities that play a major role in whether fraud may actually occur even with the presence of the other three elements" (David T. Wolfe and Dana R. Hermanson, "The Fraud Diamond: Considering the Four Elements of Fraud," *The CPA Journal*, December 2004). This additional component is worthy of additional attention because, as Wolfe and Hermanson point out, opportunity opens the door to fraud. Perceived pressure and rationalization lead the potential fraudster to the doorway, but capability leads that same person to go through the door and commit fraud. Capability is best illustrated through four personal traits:

- The employee has an authoritative position or function within the organization.
- The employee has the capacity to understand and exploit accounting systems and internal control weaknesses, possibly leveraging responsibility and abusing authority to complete and conceal the fraud.
- The employee has the confidence (ego) that she will not be detected, or, if caught, that she will talk herself out of trouble.
- The employee has the capability to deal with the stress created within an otherwise good person when she commits bad acts. (Jack W. Dorminey, Arron Scott Fleming, Mary-Jo Kranacher, and Richard A. Riley, Jr., "Beyond the Fraud Triangle: Building Better Models for Fraud Prevention," *The CPA Journal*, July 2010).

An office manager who is singularly responsible for handling the financial responsibilities of a small business implicitly assumes an authoritative position and certainly has the capacity to exploit the accounting system and internal control weaknesses. The other two traits are more personal and less a function of individual responsibilities within the business.

Since many employees are under financial pressure and have the ability to rationalize, the most effective way to deter fraud is by eliminating opportunity, accomplished by implementing internal controls.

Accidental Fraudster or Predator?

The fraud triangle and the fraud diamond both reflect the actions and characteristics of what is thought of as an "accidental" or "common" fraudster. In "Beyond the Fraud Triangle," Dorminey et al. indicate that "the common fraudster is usually depicted as having the following characteristics: first-time offender; middle-aged; well-educated; trusted employee; in a position of responsibility; and considered a good citizen through service works at the office, in the community, or at a charitable organization. This individual succumbs to pressure; develops one or more fraud schemes, and commits some fraud act." What can be more difficult to prevent or detect, however, are the fraudulent acts of a predator—a term used to refer to an employee who often begins scheming as soon as he is hired, has committed fraud before and gotten away with it, and only needs opportunity (not pressure or rationalization) to commit fraud. For these reasons, the predator may be more difficult to detect and prevent. In fact, Dorminey et al. further explain that predators "are far more deliberate than the accidental fraudster; they are better organized, have better concealment schemes, and are better prepared to deal with auditors and other oversight mechanisms." To better prevent hiring a fraudster or predator in the first place, the small-business owner should conduct background checks on potential hires and conduct reference checks with previous employers. Most importantly, the small-business owner should implement some internal controls and owner oversight to protect his business.

Internal Controls and Owner Oversight

Internal controls can help prevent or detect fraud even when limited staffing and funding render the proper separation of duties impossible. In addition, internal controls can prevent or detect errors that sometimes happen despite lack of intent to deceive or commit fraud. Small businesses, often unable to have proper separation of duties, are heavily reliant on detection controls, which take the form of reviews by the owner of payroll, cash disbursements, canceled checks, bank statements, and many other important owner oversight activities that are further explained below. A checklist is provided in the *Exhibit* to summarize key areas of internal controls and owner oversight. Small-business owners can consult with a CPA for specific internal controls pertinent to their business in addition to implementing the suggestions in this article.

The best thing a small-business owner can do to protect her business from fraud

or errors is to engage in active oversight of the accounting functions. While a small-business owner may find it difficult to be involved in the day-to-day accounting functions, mere personal oversight of the functions will often provide some protection from fraud. Although many small-business owners believe they are better off spending their time putting out fires or performing the service of their business, even minimal oversight of the accounting functions can provide some important control—or impression of control—that will benefit fraud prevention.

EXHIBIT
Internal Controls Checklist

Cash	All checks approved/signed by owner
	Receipts deposited timely
	Complete or review bank reconciliation
	Review electronic payments on bank statement
	Checks kept in secure location
Payroll	Verify employee exists
	Check that gross and net pay seem reasonable
	Monitor holiday and sick leave
	Monitor payroll tax deposit amount
Inventory	Inventory securely controlled as much as possible
	Use only approved vendors
	Inventory purchased is required for business
	Inventory is counted and verified to records at least quarterly
	Match invoice use of inventory to jobs
Vehicles	Vehicle miles are tracked
	Expenses are monitored
	Vehicles are secured and access controlled
Accounts Receivable	Credit issued to approved customers only
	Owner oversight of Accounts Receivable balances
	Bills are mailed regularly for outstanding balances
	Invoices are checked for missing invoices
	Manual invoice amounts are compared to amounts on system
	Voided invoices are marked and maintained
	Owner approves/records all accounts receivable write-offs
Accounts Payable	Use only approved suppliers
	Verify goods received before paying
	Late fees are not being paid, bills are paid timely
Expenses	Expense is a valid business expense
	Expense amount is reasonable
	Expense is properly incurred
General	Policies and procedures indicate fraud is not accepted
	Budget is prepared
	Revenues and expenses are compared to budget
	Reports of voids, adjustments, journal entries reviewed
	Computer access is limited (locked room or passwords)
Hiring	Background checks performed on potential employees
	References checked on potential employees

Most small-business owners place a lot of trust in the employees they hire. While trust is a positive thing and can enhance working relations, the small-business owner must also maintain some skepticism, which will allow him to assess employees without being too critical, offensive, or overly trusting. A little time spent each day or each week checking various accounting functions will pay dividends for the small-business owner who finds his time is constrained. In addition, accounting oversight by the owner can offset some of the deficiencies in internal controls resulting from the inability to hire enough staff in order to have full separation of duties.

For oversight, the small-business owner should analyze the financial statements on a consistent, periodic basis, such as at month-end. The owner, even with limited understanding of accounting, can compare current financial statements to prior periods or to budget in order to look for unusual variances, that is, differences from expected results. The variances can be addressed with the office manager to ensure that the accounting behind them is being handled correctly. To make the comparisons, the small-business owner should first prepare a budget. The comparison of actual balances to budgets can provide for better control of revenues and expenditures. The owner can also periodically compare revenues and expenses to prior periods, again looking for variances and then investigating and questioning those variances. Most accounting software packages can easily generate reports, which allow for financial comparisons of current balances, prior-period balances, or budgeted amounts. Finally, the small-business owner should have enough familiarity with the accounting software to periodically assess voids, deletions, adjustments, journal entries, or other similar transactions that would allow the bookkeeper to commit fraud by covering up (e.g., deleting) transactions.

Virtually all small businesses utilize information technology, especially accounting software packages, such as QuickBooks or PeachTree. If possible, access to the office where computers with the accounting software are kept should be limited. Whether that is possible or not, a good

internal control is to make sure that user IDs and passwords are utilized so that access to the accounting system is limited to those with proper authority. Passwords should be changed periodically and should include a combination of numeric, alphanumeric, and other characters for the best protection against unauthorized access. The business owner should be responsible for assigning user IDs. While this obviously will not prevent fraud by the office manager, it will eliminate or reduce fraud from being perpetrated by other employees who may have access to the office and the computer after hours. Also, a backup copy of the system should be made periodically, at least once a week. If many transactions are entered in the accounting system on a particular day, it is best to make a backup that day in addition to the weekly backup schedule. A current copy of the backup should be kept onsite and an additional copy kept offsite, and they should be rotated each time a new backup is made. The bank utilized by the business may agree to keep a backup copy or the owner can keep a backup copy at his residence.

Suggested Internal Controls

There are many internal control activities a small-business owner can implement to reduce the time involved and yet still provide the necessary checks, balances, and protection of business assets. Control activities include authorizations, approvals, and procedures put in place to reduce risk. Specific internal control activities for financial transactions in a small business are presented below.

Cash. The asset most at risk, for obvious reasons, is cash. Because of the ease with which cash can be stolen, it is one of the key areas to address with internal controls and owner oversight. Small-business owners should restrict signature authority on bank accounts to themselves and not delegate this responsibility to the office manager. Before signing checks for vendor payments, small-business owners should review all invoices and make sure the checks are written for original invoices only; paying from original invoices only will help prevent duplicate payments. Also, the business owner should check that each invoice comes from an approved vendor, compare the amount of the check to the amounts on invoices, and ensure that the items purchased are necessary and eligible expenses. The business owner should also check that bills are being paid timely so that late fees or penalties are not incurred. This can prevent wasting funds on late fee payments.

If there is more than one member of the office staff, the duties related to cash should be separated. For example, if there are two employees handling office duties, one should open the envelopes for payments and make a list (remittance advice) and the other should make the deposit. In addition, the one making the deposit should not be the one who reconciles the bank account. It is typical in small business for there to be only one person responsible for all cash transactions. Because of this, the owner should take on the responsibility of reconciling the bank account. If this is not feasible, the owner should at least check the reconciliation report prepared by the office manager each month, including a review of the original bank statement and all transactions for the month.

On the other hand, the owner could instead request that this service be performed by his CPA or tax professional. If the owner is not actually preparing the bank reconciliation each month, the office manager should be aware that the process is being reviewed by the owner. An alternative to the owner reconciling the bank account each month is for the owner to reconcile at least one month on a surprise basis. Either way, the bank statement should be reviewed for any electronic payments, because they would not necessarily be part of the aforementioned disbursement review when signing checks and approving invoices for payment. The owner should review support for payments made electronically to ensure they are valid expenses of the business and not personal expenses of the office manager or other employee. Outstanding checks and deposits should also be reviewed, especially if they are old.

Payroll. Another function of oversight and control activities that a small-business owner should monitor due to the possibility of theft is payroll. A common scheme in payroll fraud is to pay "ghost" employees—that is, employees who do not actually exist but are written a check that is then typically mailed to a postal box owned by the fraud perpetrator. In a small business, this form of fraud is much more difficult to carry out because the small size of the business virtually eliminates the chances that the owner would not recognize a check made out to an employee he had not hired. A form of payroll fraud more prevalent in small businesses is for the office manager to pay more than the approved salary. This can be done by also increasing the amount of federal withholding so that it later gets reimbursed to the employee when she files an income tax return. Increasing the amount paid and the amount withheld would result in a net payroll disbursement that is relatively similar to what it should have been and would be virtually undetectable if only reviewing paychecks. To prevent this, the small-business owner should review each paystub for gross pay, deductions, and net pay before signing payroll checks. Also, the owner should be aware of average tax deposit amounts in order to notice any unusual increase and verify that the cause was legitimate.

There are many internal control activities a small-business owner can implement to reduce the time involved and yet still provide the necessary checks, balances, and protection.

The owner should also, on occasion, check the timecards to ensure employees are only being paid for the hours they worked. Another way that an office manager or other employee could "steal" from the business is by being paid for more vacation days than are approved. Because the small-business owner may not work in the office all the time, it might be difficult to keep track of vacation days taken by the office manager or other employees, especially if taken a day at a time. The owner should maintain some form of record to ensure employees are not getting paid for more days than allowed. This entails some combination of trust and skepticism. Finally, before signing payroll

checks that include reimbursement for expenses, the owner should make sure that original receipts or invoices are submitted, that the item is an eligible business expense, and that it could not have been charged directly to the business for separate payment to the vendor rather than to the employee.

Inventory. Another item susceptible to theft is inventory, whether inventory of items for sale or inventory of assets of the business (not available for sale but used in the business). Items for sale can be stolen and therefore not generate sales revenue. Items for sale by a service business should be kept secure in a locked room when possible. Items to be sold outside the business, such as on service trucks, should be checked out to individuals responsible for selling the items to increase accountability. Also, while it can be time-consuming, a physical inventory should be conducted at least once per quarter, if not monthly, and reconciled to the inventory on the system, if applicable. Any discrepancies should be investigated immediately. Without this type of control, there is more opportunity for an employee to steal items that should be sold and recorded as sales. Inventory of assets of the business should be recorded, tagged when possible, and accounted for on occasion.

Travel and fleet expenses. Reimbursing employees for travel can provide opportunities for fraud as well. Small businesses that own fleet vehicles for business use should put some controls in place while still maintaining some level of personal oversight as well. One way to control fleet expenses is to use a fuel vendor that can provide monthly charge card reports for each vehicle. In order to generate the reports each month, the servicemen must input their vehicle number and beginning mileage before putting gas in the vehicle; this will allow the fuel vendor to generate a report that shows mileage per vehicle. If the mileage for any particular vehicle varies significantly during the month, the report should be investigated. This could indicate that the gas card is being used for personal use, either filling up a personal vehicle or making personal purchases such as for food and snacks. The owner should review the monthly vehicle reports and related statements for purchases to ensure the charge cards are not being used improperly.

Accounts receivable. Another area of susceptibility for fraud in a small business is accounts receivable, concurrently with cash. Accounts receivable means that customers will be sending in payments to the business; these payments are susceptible to fraud. Because invoices are sent to customers and related payments are subsequently received, it is important to use preprinted, numerical invoices. To ensure that all invoices are entered in the accounting system and payments received, the owner should occasionally check for missing invoice numbers. If an invoice is voided for legitimate reasons, it should be marked as void and the original should be retained in a file. If there are missing invoice numbers, the missing invoices should be investigated. If they have been voided, the voided invoice file should be investigated first. If the invoice is not there, one should follow up with the employee responsible for the particular invoice. If multiple employees are responsible for invoicing (such as in a service environment), invoices should be checked out according to invoice numbers and a checkout log maintained. Ideally, the office manager or owner should check the invoices out to each employee and record the sequence of invoice numbers on the log. The employee should sign the log indicating he received the invoices so that they can be traced back later, if necessary. This also makes the employee accountable for those invoices and reduces the opportunity to commit fraud.

Allowing an office manager to make adjustments to accounts for any reason, particularly for bad debts, is a bad internal control and provides opportunity.

In addition, many small businesses have employees who manually enter information on invoices, including a copy for the customer and a copy for the office manager, to track sales. Often, the office manager will then enter the invoices into the accounting system. As a control, the owner should periodically compare hard copies of invoices to the invoices entered in the system to ensure they are input for the correct amount. If they are entered into the system for an amount that varies from the amount on the hard copy, this could indicate the office manager is keeping the difference when the payment is received. Also, missing invoices could indicate that payments were intercepted and the funds used for personal reasons rather than being input into the system. This could be done by voiding or deleting the invoice and stealing the related payment, rather than depositing it in the business's bank account. Voiding the invoice eliminates an outstanding receivable on the system that will never be collected and helps the fraudster avoid detection.

Another internal control is to periodically assess accounts receivable for potential fraud or errors by reviewing the outstanding accounts receivable report. Accounts greater than 30 or 60 days should be assessed to determine why they are still outstanding and they should be followed up on. As mentioned earlier, voids or adjustments should also be reviewed. An easy way to steal cash is to enter the invoice and then later void or adjust the invoice amount so that it nets to a lesser amount or zero. This would prevent the invoice from showing up on the missing invoice listing, yet provides the opportunity to keep the related payment for personal use. Many accounting software packages provide an audit trail that allows the owner to see all voids, edits, adjustments, or similar transactions; this can make it easier to detect voided or adjusted invoices.

Write-offs of accounts that are deemed uncollectible should only be processed by the owner. Allowing an office manager to make adjustments to accounts for any reason, particularly for bad debts, is a bad internal control and provides opportunity and enhances capability for theft. Another internal control that can be implemented to check accounts receivables is to send statements to all customers that have had transactions during a certain period. If payments were being intercepted, the customer is likely to call and indicate they had previously made payment, which might help the owner

detect fraud. Granted, there is the possibility that the office manager may intercept the call, but it is still a control that may prove worthwhile and could reduce the capability trait of confidence that the fraudster will not be detected.

Information and communication. An important concept of internal controls is information and communication. Information and communication can be implemented through policies and procedures. Small-business owners should have a policy in place indicating that fraud will not be accepted and will be prosecuted. It is important to share the policy with employees and make sure they are aware of its existence. If fraud is committed, it is important to follow up and prosecute it so that employees know that the owner stands behind the policy. If employees believe they will not be prosecuted for fraud, they are more likely to submit to perceived pressure and capability and commit fraud, given the opportunity.

A Worthwhile Effort

Most of the suggestions offered have been to address the opportunity component of the fraud triangle. This is certainly the component that the owner can most assuredly address through a combination of internal controls and personal oversight of accounting functions; however, the small-business owner can also affect rationalization by making employees feel valued and by encouraging loyalty to the business. Employees who feel valued and appreciated are less likely to rationalize theft and commit fraud from their employer. This can be achieved by treating employees well and compensating them appropriately, including bonuses or raises.

While it may seem very time-consuming to incorporate internal controls in a small, private business, the efforts will be worth the time and money involved. Small businesses are susceptible to theft because of the limited staff responsible for accounting functions. Therefore, owners should work to implement internal controls and be more involved in the finances through active oversight. Any oversight by the small-business owner of the accounting functions makes it less likely that fraud will occur.

Even in the absence of actual internal controls, the perception that an owner is checking up on business operations will serve as a deterrent for many. A CPA can help incorporate internal controls in small businesses and provide specific guidance on oversight activities that can keep employees from committing fraud. The cost involved may be one of the best investments a business owner makes. ❑

Linda A. Kapp, EdD, CPA, *and* ***Gordon Heslop, DBA, LLB, CMA, CIA, CFM,*** *are assistant professors of accounting, both at the college of business and technology of Texas A&M University–Commerce, Commerce, Texas.*