Small business fraud and the trusted employee

Protecting against unique vulnerabilities
Small businesses have it rough. They’re particularly vulnerable to fraud because they lack the resources to implement complete systems of internal controls and properly segregate accounting duties among their limited staffs. However, small businesses don’t have to be rife with fraud. Here are some viable prevention options.

Bob and his brother, Bill, owners and operators of Acme Tractor for 30 years, were close to retirement. A local bank had continually financed Acme, which had an inventory of farm tractors worth millions of dollars. The owner’s wives, Jane and Julie, shared accounting duties in the company. Jane would approve invoices. Julie would prepare the checks and either Bill or Bob would sign them. The receipt and payment cycle included a series of checks and balances with no one employee responsible for the entire cycle.

Jane and Julie retired from the business, and James, Bob’s son, assumed the bookkeeping responsibilities. James, 30, had been working in various jobs at the business since high school. Now the brothers entrusted him with all aspects of bookkeeping for the business: accounts payable, accounts receivable, payroll, and all account and bank reconciliations. They gave him check-signing ability and a business credit card.

Soon after becoming the bookkeeper, James married and began a family. As his personal monthly bills increased, he found it difficult to maintain the lifestyle he had known when he was single and living with his parents.

The fraud scheme began simply. At first, James began illegally using his business p-card (or purchasing card) for small personal expenses, such as gas for his personal vehicle and fast food meals. After several months, his charges for personal expenses increased in number and dollar amount, including charges for taking out his wife and children to fine restaurants, clothing for himself and his family, and even high-end electronic products. No one at Acme noticed the continual increase in charges for personal items because James controlled all payment checks to the credit card company.

James’ fraudulent activities expanded. He began embezzling from the payroll system. Because he was a manager, he didn’t have to use the time clock and began to pay himself for excessive overtime pay. He would give himself paychecks in lieu of not taking vacation time, even though he took all his vacation days. Acme management was still oblivious.

He then began writing checks payable to himself, but he would write a regular recurring vendor’s name on each check stub and hand-key it into the computer system. When the bank statements came each month, James would alter the images of the checks on the statements to match the vendors on the check stubs and in the system. Then he would hide evidence of the fraudulent checks he had cashed by photocopying the altered pages of the bank statements and shredding the original statements.

Crafty James wasn’t done yet. He opened a new personal credit card at the business’ bank. Now it was easy for him to electronically make bank drafts for paying the business’ monthly credit card statements and then write company checks to pay his personal card. If anyone reviewed the check stubs, it would only appear that one credit card invoice had been paid each month. James could charge the company’s credit card for his personal expenses and charge additional purchases to this new credit card. He used company funds to pay off both cards. Sweet deal.

Some fraudsters rationalize their thefts as “temporary” loans they will repay later. James executed his frauds without any intention of returning the money. His thefts from the company for 2½ years were large enough to create company cash flow problems.

One of James’ cousins accidentally discovered the crimes in December 2010 when he was searching the business’ online banking system for a canceled check and discovered that several checks in one month had been payable to and signed by James. Management didn’t contact law enforcement nor engage an outside accountant. During its internal investigation, the family determined that it had lost at least $60,000 (though it was probably quite a bit more than that). Family members confronted

By G. Stevenson Smith, Ph.D., CPA, CMA; Theresa Hrncir, Ph.D., CPA; and Stephanie Metts
James. He confessed and explained how he had stolen the money. The business fired him after he signed an agreement for restitution, which stipulated that the family wouldn’t prosecute.

Before they discovered James’ crimes, Bill and Bob had attributed cash-flow problems to a downturn in the economy. And James, of course, concurred. The brothers had to lay off employees and cut or reduce employee benefits for both family and non-family employees. The company still hasn’t recovered from James’ fraud schemes.

Small businesses are particularly vulnerable to fraud because they lack the resources to implement complete systems of internal controls and properly segregate accounting duties among their limited staffs. Therefore, accounting personnel may be tasked with completely inappropriate job functions that provide easy opportunities for committing financial frauds. Furthermore, the business cultures of small businesses are developed around a concept of a “trusted family” of employees. Consequently, placing trusted employees in positions without proper internal controls doesn’t appear to be an unreasonable decision to managers of a “family” business.

According to the ACFE’s 2012 Report to the Nations, estimated median losses for small organizations — those with fewer than 100 employees — that experienced a fraud were $147,000 (ACFE.com/RTTN). The report indicated that small organizations are the most common victims in fraud instances at 31.8 percent — the highest rate of any business size category. (For example, organizations with 100 to 999 employees had a fraud incident frequency of 19.5 percent; 1,000 to 9,999, 28.1 percent; and 10,000 plus, 20.6 percent.)

The five most common fraud schemes for organizations with fewer than 100 employees in the ACFE report were: billing fraud, corruption, check tampering, skimming and expense reimbursement fraud. Corruption schemes deal with crimes such as bribery, illegal gratuities and kickback arrangements. The largest number of perpetrators in the entire study, 41.5 percent, had been with the organization between one and five years, most of them had a college degree and worked in the accounting area.1

Even using ACFE survey data, it’s difficult to estimate the true losses from employee frauds. Small businesses often don’t report these crimes because of families’ embarrassment, decisions not to file criminal charges or wanting to keep knowledge of the crimes privy. Only a small number of small business embezzlement victims — roughly two percent — report crimes even though 40 percent of small businesses report they have been victimized, according to the May 16, 2011, article in The Daily Record, “Employee theft at small business high and hard to detect,” by Kathleen Johnston Jarboe (http://tinyurl.com/byozj4w, accessible for a fee).

In this article, we provide several practical recommendations for small business managers to help them prevent these fraud schemes.

The trusted employee
Employee thieves normally don’t fit the stereotypical career criminal profile. They often are in good standing, have worked with a company on average of four to five years and nine out of 10 of them are first-time offenders, according to the January 2011 article, “Opportunity Knocks,” by Brian Shappell in Business Credit magazine (available only to NACM members, http://tinyurl.com/b2t2rbr).

Approximately 87 percent of the occupational fraudsters studied in the ACFE’s 2012 Report to the Nations had never been charged or convicted of a fraud-related offense, and 84 percent had never been punished or terminated by an employer for fraud-related conduct. Consequently, the most trusted employee — who has easy access to funds and has never stolen anything — may yield to the overwhelming temptation to take company resources when he or she is faced with personal financial stress. Donald R. Cressey’s well-known fraud triangle highlights factors such as personal stress (what he called “perceived non-shareable financial need” or pressure) that contribute to the implementation of a fraud scheme. (He said the other two points of the triangle are perceived opportunity and rationalization. See the ACFE’s 2012 Fraud Examiners Manual, 4.502 – 4.504.)
The motives for committing a financial fraud include greed, financial pressures or employee disenfranchisement. Disenfranchised employees become resentful after spending years handling mundane details for their employers without recognition, according to “The Downside of Good Times,” by Anita Dennis in the November 2000 issue of Journal of Accountancy (http://tinyurl.com/ayfrsws). They feel forgotten.

Other employees are motivated because they believe they’re entitled to more financial compensation. They also rationalize they’ll only “temporarily” borrow the money, and they’ll return it later. Motive, rationalization and opportunity work in combination to increase the potential for employee fraud in any organization.

In many small businesses, the major reason fraudsters can commit their crimes is because management trusts them so much; they’re family members or longtime friends, or they have proven work records and years of service, according to “The Trust Factor,” by George A. Cassola in the Managerial Auditing Journal, volume 8, 1993, issue 7 (http://tinyurl.com/bzdkc3w). That high trust level enables fraudsters to hide their activities. Even when business owners find suspicious behavior, they often believe it’s inconceivable that employees would violate these trusted relationships. So, consequently, they hesitate to investigate, which results in much larger frauds.

Telltale signs of employee theft
Many times, we can see red flags that an employee might be susceptible to committing a fraud or is already involved in fraudulent acts. The ACFE’s 2012 Report to the Nations identified the top two behavioral red flags as living beyond their means (36 percent of all 1,388 cases) and experiencing financial difficulties (27 percent). Additional behavioral red flags that complete the top five include: unusually close association with vendor/customer, control issues and unwillingness to share duties, and divorce/family problems.

KPMG collected data on 348 fraud cases for its 2011 “Analysis of Global Patterns of Fraud: Who is the typical fraudster?” (http://tinyurl.com/ab8kz55). Its findings identified characteristic red flags, such as self-interest, tendency to bend rules, confrontational attitude when challenged, refusing a promotion or a vacation and delay in producing reports.

We have to be careful when we find red flags of employee fraud. Many employees experience stress and financial setbacks in their lives, and they don’t defraud their employers. Yet when you identify an employee who shows certain behavioral signals, it would be worthwhile to be especially attentive to that employee’s activities. You may need to analyze that employee’s job responsibilities to understand what occurred.

Traditional fraud schemes in small business
Regardless of an organization’s personal connection to an employee, allowing one employee uncontrolled access to the financial records without verification is comparable to giving a bank robber the combination to the bank vault. The Acme fraud case is an example of a typical fraud that occurs in many family businesses — and many other small entities — because of misplaced trust and no control procedures. (We prepared the actual Acme case with the help and permission of the family. We’ve changed only the participants’ names.)

The ACFE’s 2012 Report to the Nations says that occupational fraud is more likely to be detected by a tip — or as we say, chance — than any other method. According to the PricewaterhouseCoopers’ 2011 global economic crime survey, 41 percent of fraud cases were detected by a combination of tips or accidents — or chance (http://tinyurl.com/yg5q2td). This was true at Acme Inc.

So, small businesses don’t necessarily uncover fraud just with internal control practices, external audits, account reconciliations, IT controls, management reviews or confessions. Perhaps excessive spending on these time-consuming processes may not always be the best choice for a small business.

However, many small business owners might go to the other extreme and believe that internal controls are an expensive luxury they can’t afford. Internal control procedures are common-sense ideas formalized to protect company assets and create a consistent set of expectations and behaviors. Even a small family company, such as Acme, had an acceptable system of internal controls before James took over all the bookkeeping functions. (See sidebar on page 47.) It’s not necessary to be a large, well-financed company to institute a minimum level of internal accounting controls with minimum costs.

Recommendations for avoiding fraud
Numerous internal control guidelines have been published for large businesses. However, the internal control needs of a small business are different than for multinational corporations, national banks and big government.

A large business will have its cash collection and deposit activities separated among numerous employees, but this isn’t always affordable for a small business. A small business, like the Acme Company, needs to concentrate on: credit card security, fidelity bonds, proper use of bank accounts, reliable reconciliations, accounting service selections and a review of corporate culture.

Credit and purchasing cards
Employees, such as James, use company credit cards or p-cards (purchase or procurement cards) to buy small-ticket items and commodities without having to go through account payable systems. Small businesses need to use merchant category codes with these cards, which will restrict their use at such locations as jewelry or electronic stores or gaming casinos, for example. Each card should have limits for amounts that can be spent daily and for

©2013 Association of Certified Fraud Examiners, Inc.  FRAUD-MAGAZINE.COM  JANUARY/FEBRUARY 2013  FRAUD MAGAZINE  45
total expenditures. Employees shouldn’t use these cards for cash advances.

Request pie-chart records of all expenditures on p-cards from credit card companies. Visual comparisons of spending patterns quickly identify irregular spending patterns.

**Bonding**
A small business should consider bonding employees who have access to accounts — especially those who have signatory authority — through an insurance company. If a bonded employee commits financial fraud, the insurance company will reimburse the company for the loss. Some contracts stipulate that the small business will prosecute the implicated employee. A more expensive alternative is crime insurance, which has wider theft coverage but doesn’t require that the small business prosecute the accused employee. The bonding process usually includes employee criminal and financial background checks.

**Bank accounts**
If your business still uses handwritten checks, keep two separate, rotating bank accounts; allow all canceled checks to clear through one account during the month while you’re writing checks through the second account. Checks from the two accounts should have distinct logos so you can differentiate them. At the end of each month, transfer the ledger balance to the second account. All checks should clear from one month to the next, and the account used in the previous month should clear to a zero balance.

Require dual signatures either on all company checks or those above a specific amount. Separately review each quarter those checks that don’t require dual signatures.

**Hire external services for reconciliations, auditing**
Hire external services for bookkeeping, internal accounting checks and audits of your firm’s records. Bookkeepers simply compile your company’s financial records; they won’t necessarily assure that the prepared financial statements will be accurate or lack gross misrepresentations.

Strengthen financial assurances related to these financial reports by hiring an external accountant or other independent organization to reconcile bank statements. Only your banks — not your management — should directly send statements and original checks to the external accountant.

External accountants can find inconsistencies by comparing semi-annually or quarterly sampled payroll transactions or vendors’ names and addresses to accounts payable information. A full audit might not uncover fraud, but it can quickly identify glaring internal control weaknesses.

The traditional argument against taking these preventive actions is “our employees wouldn’t steal from us,” and they don’t … until they do. So, it’s important for small businesses to pay out the cash for external accounting services, or they could be paying a lot more to clean up messy fraud. Or even worse — the business might have to curtail operating activities because of a lack of cash flow. And it can face the erosion of bank credit lines plus increasing interest rates because of its lending risk for banks.

Beyond these measures, owners and managers, of course, as always, need to set the tone for honesty and integrity in their daily activities. If they don’t publicly adopt the standards they impose on their employees, then deceitfulness will be embedded into the organization’s culture. Shortcuts and loosely controlled expenditures by the management are unacceptable.
Small but mighty
Small businesses have it rough. They constantly have to watch expenses and cash flow on tight margins. And they’re particularly vulnerable to fraud because they lack resources to implement complete systems of internal controls and properly segregate accounting duties among their limited staffs. However, they can use some viable options — even if they’re financially constrained — to be small but mighty.

G. Stevenson Smith, Ph.D., CPA, CMA, is the John Massey Endowed Chair and professor of accounting at Southeastern Oklahoma State University. His email address is: sgsmith@se.edu.

Theresa Hrncir, Ph.D., CPA, is a professor of accounting at Southeastern Oklahoma State University.

Stephanie Metts is a special assistant in the School of Business at Southeastern Oklahoma State University.

1 According to an analysis of 1,000 major embezzlement cases from 2007 through 2010, 60 percent of the perpetrators were employees with finance/bookkeeping responsibilities. See “Small Businesses Face Greatest for Fraud & Embezzlement,” by Christopher T. Marquet, Dec. 7, 2010, http://tinyurl.com/azjra4l. © Marquet International Ltd.

Internal controls were fairly good, before James took over

Acme Tractor, the actual family small business profiled in the article, had been operating well for 30 years, until James — the son of one of the owners — assumed the bookkeeping responsibilities. He then began to rob the company of at least $60,000 in 2½ years. But let’s harken back to better times when we could study the company for good small-business internal controls.

The owners were brothers, Bob and Bill. Their wives, Jane and Julie, shared accounting duties in the company. Jane would approve invoices. Julie would prepare the checks and either Bill or Bob would sign them. The receipt and payment cycle included a series of checks and balances with no one employee responsible for the entire cycle.

Jane would open the mail, log the payments and give them to Bob to make the deposit. Julie would post them to the general ledger. Bob usually reconciled the bank statements.

The company’s accounting firm would compile the financial statements based on the data that Acme supplied. Acme didn’t commission any audits of the financial records. See the system of checks and balances in the cash receipts and payments cycle in the diagram below.

Owner:
1. Reconciled bank statements.
2. Authorized payments.
3. Made bank deposits.

Jane:
1. Opened mail; collected and recorded received checks into company log book.
2. Approved invoice payments.

Julie:
1. Posted checks and cash received into general ledger books.
2. Prepared outgoing checks for invoice payments.

Checks and invoice sent to owner for authorization and signature.

Original checks and cash.

Completed vendor’s invoice sent for payment.

Acme’s cash receipts and payment cycle