Business Horizons (2015) xxx, xxx—xxx

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

ACCOUNTING MATTERS

# Fraud risk management: A small business perspective

**Megan F. Hess** [a,*], **James H. Cottrell Jr.** [b]

[a] *Williams School of Commerce, Economics, & Politics, Washington and Lee University, Lexington, VA 24450, U.S.A.*
[b] *Partner, Forensics, Deloitte Financial Advisory Services LLP, Washington, DC 20004, U.S.A.*

**KEYWORDS**
Small business;
Organizational ethics;
Fraud;
Misconduct;
Risk management

**Abstract** Small businesses face big challenges when it comes to managing fraud risks. Financial strain, rapid growth, and a lack of resources and expertise create ample opportunity for motivated fraudsters to take advantage of small businesses. In this article, we draw upon insights from our years as fraud investigators to offer seven practical recommendations to help small business leaders prevent and detect fraud in this unique environment. These strategies can help even the smallest company make a big difference when it comes to fraud risk management.


## 1. Introduction

Small businesses provide the backbone of the American economy. According to a 2014 report by the U.S. Small Business Administration, businesses with fewer than 500 employees employ 48.5% of private-sector workers, provide 63% of net new private-sector jobs, and produce 16 times more patents per employee than large firms (SBA, 2014). Unfortunately, this important segment of our economy is also one of its most vulnerable. According to a 2014 survey by the University of Cincinnati, 64% of small businesses have been victimized by fraud (Kennedy, 2014). What is even more concerning than the rate of fraud in small business is its far-reaching impact. Recent research suggests that companies lose roughly 5% of their revenues to fraud each year, and fraud is a significant contributing factor to small business failure (Association of Certified Fraud Examiners, n.d.). The total cost of fraud, however, cannot be measured in dollars alone. Fraud also takes an emotional toll on its victims, diminishing worker productivity and morale.

Making small businesses more resilient to fraud could provide real benefits to their owners and to the overall economy, but small businesses frequently lack the resources and the expertise to fight fraud. In this article, we explore the unique challenges and opportunities facing small businesses when it comes to fraud risk management. As fraud investigators, we have seen these struggles firsthand, and we empathize with small business owners' despair when they unwittingly find themselves a victim of a fraud. Drawing on our experiences in the

* Corresponding author
*E-mail addresses:* hessm@wlu.edu (M.F. Hess), jhcottrell@deloitte.com (J.H. Cottrell Jr.)

0007-6813/$ — see front matter 
http://dx.doi.org/10.1016/j.bushor.2015.09.005

field, we offer seven practical recommendations for small business leaders to help them strengthen their defenses against fraud risk and build more ethical organizations.

## 2. The small firm perspective on fraud risks: Unique challenges and opportunities

Small businesses may find themselves victimized by fraud in myriad ways, but the most pervasive threats come from four sources: customers, vendors, employees, and the Internet. In the following paragraphs, we describe the typical fraud schemes associated with these four threats to help small business leaders become more aware of their fraud risks. While these examples are not an exhaustive list of fraud threats, they provide a framework and a launching point for small business leaders to begin to evaluate their own vulnerabilities.

Customers victimize small businesses by stealing inventory (shoplifting), passing bad checks, or making false claims for refunds, returns, and warranties. Customer-related fraud threats are especially pervasive in the retail industry. In fact, a 2013 study by *Business Insider* estimates that American retailers lose $45 billion each year to retail theft. Small businesses across all industries can also be hurt by customers who take advantage of small businesses by being 'slow payers' or who require unreasonably high levels of service. While not necessarily frauds, such unethical customer behavior can put undue strain on the business's scarce resources.

Vendors, often with the assistance of an insider, can orchestrate large scale, difficult to detect frauds against small businesses by using shell companies, overbilling for services, and paying bribes to secure contracts. Vendors can also take advantage of small businesses by stealing their intellectual property, their customers, and their top talent. Because small businesses often lack the resources and the expertise to install the necessary security and legal protections to deter these customer- and vendor-related frauds, criminals take advantage of the opportunity to exploit what they see as an easy target.

Employees, on the other hand, may find very different motivations for committing fraud. While some may steal from their employers out of greed or need, they may rationalize their behavior as a right that they have earned through their hard work and sacrifice on behalf of the business. Small business employees may feel a sense of entitlement to the company's assets when they have played such a prominent role in building them up. Employees may also rationalize stealing as merely a temporary loan and justify their actions with the good intentions to pay everything back before it is missed. Employee-related frauds may take on many forms ranging from the theft of company assets to revenue skimming, purchasing card and expense reimbursement abuse, time theft and other forms of payroll fraud, and even complex schemes to divert company funds through shell companies or kickback arrangements with vendors. Unfortunately for small businesses, employee-related frauds are on the rise. A 2009 survey by PriceWaterhouseCoopers reports that 76% of economic crimes against U.S. businesses were committed by insiders.

Increasingly, criminals are also exploiting weak cyber security measures at businesses both large and small to steal vast amounts of confidential customer information through the Internet. Data breaches sometimes occur through sophisticated software hacks, but criminals can also lure small business employees into voluntarily sharing this lucrative information through phishing scams. Criminals have also been known to sift through the trash ('dumpster diving') or to pose as a customer, vendor, or government official to steal business account records and other private information. Internet fraud and other threats to data privacy are especially worrisome for small businesses now that 45 states have passed laws that hold businesses accountable for data breaches perpetrated by third parties.

All of these sources of fraud risk have one element in common—exploiting opportunity. How can small businesses reduce this opportunity and build up their defenses against fraud? To start, small business leaders need to become more aware of the unique challenges and the unique advantages facing their particular operation. In addition to the many fraud risks elaborated here, small business leaders should gather a diverse group of trusted advisors to help them brainstorm other ways that their business may be vulnerable and to help them discuss ways to mitigate these threats. While the task may seem overwhelming from the outset, small business leaders should take heart that despite these many challenges and vulnerabilities, small businesses also present a unique opportunity when it comes to building a more ethical organization. Large, established companies often struggle to maintain a cohesive ethical culture. Small businesses, on the other hand, may use their smaller size to an advantage by enjoying more clarity in their messaging and values. Small businesses also excel at community engagement; indeed, small business leaders provide the backbone for local philanthropy, civic leadership, and community development. These local ties may allow small business leaders to work together to

spread awareness of fraud threats and develop innovative approaches to reducing fraud risks. Small businesses are also distinguished from their larger peers by the close, personal nature of their business relationships. Small business owners often leverage family and friends to fund, staff, and grow the enterprise, and while these connections can bring their own ethical challenges, they also give small business owners a 'trust advantage' over their larger competitors.

The important question for small business leaders, then, is how to best leverage the advantages of being small when it comes to fighting big challenges like preventing and detecting fraud. Below we offer seven practical, affordable recommendations for managing fraud risk in this unique environment. These strategies can help even the smallest company make a big difference when it comes to fraud risk management.

## 2.1. Show that ethics matters

It goes without saying that ethics is important and that most companies are run by good people. So why do small business leaders need to be more explicit about the importance of ethics? Isn't this just stating the obvious? Research shows that, in fact, ethical issues are *not* always obvious in a business setting. Thinking in business terms tends to crowd out and minimize ethical issues such that employees are often unaware of the moral implications of their actions. Focusing on business or financial matters tends to narrow perceptions and emphasize cost-benefit calculations in such a way that ethical issues are unconsciously ignored or discounted in the decision-making process. When coupled with the unique situational challenges that make small businesses especially vulnerable to fraud, the lesson is clear—small businesses cannot take ethics for granted.

Fortunately, there are many things that small business leaders can do to bring ethics back into the foreground by showing that ethics matters in their organizations. The first rule of thumb is that every time a leader talks about profits or efficiency, he or she should also explicitly state the importance of meeting these goals through ethical means. . . every time! It should *never* go without saying that ethics matters. Leaders may also find it useful to probe decision makers in their organization with the question, "What's the right thing to do here?" Employees can display incredible ingenuity when coming up with creative ways to solve business ethics problems, but they may hesitate to voice these solutions without explicit permission from company leaders.

Small business leaders can also show that ethics matters by writing and championing a code of conduct written in simple, non-legal terms, which aligns with the company's mission and values (see www.ethics.org for some great, free resources on writing an effective code of conduct). Good codes of conduct not only limit misconduct but also inspire exemplary behavior. Small business leaders can go one step further with their codes and extend these principles to govern their relationships with their suppliers, too. Signaling the importance of ethics in these ways not only increases employee sensitivity to ethical issues and encourages them to speak up when they see problems, but it also prevents fraud by screening out employees and business partners that are uncomfortable with the level of emphasis put on ethical behavior by the company.

## 2.2. Make reporting easier

Small business leaders who think that an ethics hotline is a luxury may be surprised by both the importance and the affordability of this communication channel. In terms of importance, facilitating the reporting of observed misconduct is the single most effective way to detect fraud. The Association of Certified Fraud Examiners (2014) reports that insider tips are responsible for catching 43% of all frauds—more than all other detection methods combined, including external audits. When it comes to affordability, the pricing for third-party hotline providers has become much more competitive in recent years, with some providers offering 24-hour-a-day phone and e-mail support in multiple languages for an annual fee of $500. Using a third-party hotline provider is preferred because it offers anonymity for reporters, which increases both the rate and quality of reporting. Third-party hotline providers also provide case management and investigation support to help small businesses deal with allegations of misconduct.

If the price point for a third-party hotline provider is too high, however, small business leaders can take intermediate steps to provide effective communication channels for reporting. Small businesses can recommend that employees and other business partners contact the company's auditor or a designated member of the board if they have concerns. This contact information should be prominently displayed with a reminder that all employees have an affirmative duty to report suspicious behavior. Small businesses can expand suggestion boxes to include questions and concerns that may help leaders identify problems early.

Leaders can also take the initiative and ask about potential problems rather than waiting for the bad news to find them. As former fraud investigators, we know that the single most important question you

can ask an employee is, ''What else should I know?'' Most employees will not take the initiative to raise a concern on their own. They may be worried about being perceived as a snitch, think that nothing will be done about it, or just not have enough to go on yet. When asked directly, however, these same employees are more than willing to share their suspicions. We have worked on several investigations where an employee had been gathering incriminating evidence on a fraudster for months, and when we asked why he/she had not said anything about it before, he/she simply replied, ''Well, no one ever asked.'' Employees that care about their organizations do want to be helpful, but their natural cautiousness prevents them from going out of their way to do so. Small business leaders can lower their fraud risk by opening up communication channels with employees so that when problems do arise, they can be identified and resolved early.

## 2.3. Trust but verify

Most frauds in small businesses are committed by trusted, long-time employees because it is easy for them to steal from their employer and cover their tracks. The problem is not so much that this trust in employees is misplaced. In fact, most fraudsters have no criminal backgrounds or history of suspicious behavior. Rather, good people often find themselves rationalizing bad choices when they are facing intense pressures in their personal lives, such as the threat of bankruptcy, a divorce, or the desire to support a loved one struggling with addiction.

Small business leaders can protect themselves from employee-related fraud threats in several ways. Simple internal control procedures like segregating duties and requiring mandatory vacation periods each year can go a long way toward preventing employee theft and detecting schemes already in place. Proper segregation of duties means that different employees are responsible for custody of assets, record keeping, approvals, and reviews. Likewise, different employees should be responsible for authorizing transactions and recording them. Common fraud schemes, like diverting company money by authorizing payments to a shell company or setting up a ghost employee, can be prevented through proper segregation of duties. Small businesses can also use technology to help them monitor employees relatively inexpensively. For instance, smartphones can be enhanced with an inexpensive security application that allows monitoring of employee location (through GPS) and uses employee fingerprint recognition to control timecard reporting and building access. Remember that the threat of detection is itself a powerful deterrent.

The 'trust but verify' approach can also help reduce the risk of frauds committed by outsiders, especially Internet fraud phishing scams. Employees should be trained to watch out for offers that sound too good to be true, and they should be required to always seek approval before sharing sensitive information with anyone, no matter how familiar or official the requester may appear. Likewise, refunds, returns, and warranty requests should follow a tightly controlled process that is carefully monitored for abuse. Small business leaders may find it difficult to apply these best practices to friends, family, and long-time customers or vendors. However, a 'no exceptions' policy is paramount when it comes to proper checks and balances. Friends, family members, trusted vendors, and loyal customers will come to appreciate and even respect an owner's vigilance if it is applied consistently and evenly.

## 2.4. Beware of the slippery slope

Small businesses can further reduce their risk of fraud by applying this no exceptions policy to enforcement of the company code of conduct. Too often leaders are tempted to look the other way when it comes to small transgressions, like abusing company sick leave, using company assets for personal benefit, or inflating expense reimbursement requests. However, small transgressions, left unchecked, pave the way for bigger problems down the road. Some mistakes that may seem immaterial can create large regulatory and compliance risks for the company, particularly when doing business in a foreign country or with a government agency at the federal, state, or local level. Failure to pay proper sales, use, and payroll taxes is a major contributor to small business bankruptcy.

Employees that get away with small violations of company policy are also more likely to commit larger transgressions in the future. They see that the company is not willing to put in the effort to hold employees accountable for violating company policy. Employees that get away with small transgressions are also able to rationalize their behavior as not that bad and lower their moral standards. Over time, the degradation in behavior and moral standards may happen so gradually that neither the employee nor his/her supervisor notices the decline.

Small business leaders should also be careful to hold all employees accountable to the code of conduct. Leaders may be tempted to overlook the behavior of a top grossing salesperson or other valuable member of the team, but such uneven application of the company code violates the principle of procedural justice and will certainly incite the ire of other employees. Otherwise honest

employees may become discouraged and less willing to toe the line. Prioritizing profits above ethics also increases fraud risk by providing employees with a rationalization for cutting corners to meet performance goals. In short, every transgression, no matter who commits it or how small it may be, should be investigated and handled judiciously.

### 2.5. Look for suspicious patterns

Small businesses may not be able to afford sophisticated fraud monitoring technology programs, but they can increase their likelihood of detecting frauds by looking for suspicious patterns and unusual transactions. Many credit card providers have built in controls and data analytics that can help to minimize the risk of purchasing fraud schemes. Simple queries of accounting database records can also identify the red flags of suspicious behavior such as a transaction posted on a holiday, round dollar amounts, payments made to vendors that have the same address as an employee, or employees getting paid past their termination date. A more sophisticated analysis applying Benford's law to a population of transactions can also identify fraud (see www.auditnet.org for useful tutorials).

If you do not have the data analytic skills—and cannot afford an intern that does—do not fret. The search for suspicious activity need not be confined to databases. Check the file drawers—missing, altered, or homemade documentation may indicate fraudulent activity. Suspicious patterns can also be behavioral rather than financial. The Association of Certified Fraud Examiners (2014) indicates that 44% of fraudsters are living beyond their means, so pay attention to surprising lifestyle changes amongst employees. Sudden personality changes, control issues, and defensiveness can also be behavioral red flags of fraud. In the frantic pace of life as a small business owner, it can be difficult to take the time to look for the warning signs of fraud, but a little bit of sleuthing can go a long way toward managing fraud risks.

### 2.6. Good outcomes are no excuse for bad decision making

Small business leaders, like all decision makers, are prone to overlook risky choices that have good outcomes. Even worse, we may consider the decision maker to be good when, in fact, he or she may have just been lucky. Psychologists call this tendency 'outcome bias,' and it represents a common source of fraud risk in small businesses. Leaders that excuse or ignore bad decision making that ended in good outcomes unwittingly send a powerful signal about what really matters in their organization, allowing an 'ends justify the means' mentality to spread. This 'whatever it takes' mentality has been cited in a recent survey conducted by KPMG (2013) as the most common reason that employees engage in unethical behavior.

Fortunately, small business leaders can take steps to mitigate outcome bias. It is important for small business leaders to bring more attention to *how* decisions are made in their organizations. Good decision making involves transparency, broad information search, playing devil's advocate to uncover logical flaws, careful testing and analysis, and validation with key stakeholders. As an added benefit, being transparent about decision making within the organization can improve processes and help develop future managers.

### 2.7. Give employees what they need to reach their goals

Finally, small business leaders can reduce their risk of fraud by giving employees the tools and resources they need to reach their goals. Without the appropriate resources to meet a stated goal, employees may resent being held to what they perceive to be an unreasonable standard and rationalize cheating or cutting corners as a necessary evil to reach the goal. When a company sets its sales goals or efficiency goals too high, it gives employees implicit permission to do whatever it takes to meet them, and we know that this attitude is the single most common rationalization for unethical behavior.

Instead, small business leaders should think carefully about setting goals that will stretch employees to do their best without breaking their loyalty by violating their sense of fairness. Moreover, if circumstances change such that an agreed upon goal is no longer attainable, leaders should step in and change the goal to reflect the new realities of the business. Research shows that financial incentives work well for encouraging high performance on repetitive, mechanical tasks, but financial rewards tend to narrow employee focus in ways that diminish performance on creative, cognitive tasks. In short, leaders should pick appropriate rewards that will foster the kinds of behavior that they are seeking without unintentionally fostering the kinds of behavior that they would like to avoid.

## 3. Developing your own fraud risk management plan

In this article we have described the four primary sources of fraud risk for small businesses and outlined

seven steps that small business leaders can take to mitigate these risks. The first step in putting together your own fraud risk management begins with an awareness of both the unique challenges and opportunities facing your particular operation. It may take a year or more to develop this awareness into a fraud risk management plan that works for your situation. As your resources and expertise change over time, so can the scope and sophistication of your plan.

We know that the very nature of small business management means that decision makers are working with few resources and often moving from one fire to the next, so setting aside the time to take stock of fraud risks and develop a fraud risk management plan is hard. Nevertheless, small business leaders should view the development of a fraud risk management plan as an important investment in the business's future. Leaders should adopt a mindset that fraud risk management is not just a challenge but also an opportunity. Small business leaders that foster a work environment full of purpose, accountability, and honesty can not only reduce their risk of fraud but also build high-performing, resilient organizations. Even with limited financial resources, small businesses can improve their efforts to prevent and detect fraud, and in doing so, unleash the full potential of their businesses.

## References

Association of Certified Fraud Examiners. (n.d.). *ACFE report estimates organizations worldwide lose 5 percent of revenues to fraud*. Retrieved from http://www.acfe.com/press-release.aspx?id=4294973129

Association of Certified Fraud Examiners. (2014). *Report to the nations on occupational fraud and abuse*. Retrieved from http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

Kennedy, Jay P. (2014). *From apathy to disdain: Why small businesses refuse to call the police when employee theft occurs*. Presentation at the Annual Meeting of the Criminal Justice Sciences, February 18-22, Philadelphia, PA. Additional information at http://www.uc.edu/news/NR.aspx?id=19231

SBA. (2014, March). *Office of Advocacy: Frequently asked questions*. Retrieved from https://www.sba.gov/sites/default/files/FAQ_March_2014_0.pdf