10 Truths YOU NEED TO KNOW ABOUT Fraud

By Bonita K. Peterson, CMA, CPA, and Paul E. Zikmund

You've undoubtedly heard about the recent corporate accounting scandals, but how much do you *really* know about fraud? Ignorance is *not* bliss when it comes to fraud because, like high blood pressure, it can be a silent killer of your company's financial health. We will look at 10 truths you should know about fraud to help reduce the risks of it occurring within your business.

1. Fraud is prevalent.

Fraud is a pervasive problem that knows no boundaries, regardless of the industry, the country, or the size of the company. For example, in a 2003 national survey, KPMG reported that 75% of organizations experienced fraud during the prior 12 months, with employee fraud the most prevalent. PricewaterhouseCoopers (PwC) conducted an international economic crime survey in 2003 and reported that 37% of respondents had discovered fraud in the previous two years. Further, the firm reported that no industry is safe since more than 30% of respondents in each of the industries surveyed reported fraud experiences. Ernst & Young conducted its third international fraud survey in 2000 and found that more than two-thirds of respondents had suffered from fraud in the prior 12 months, and almost one in 10 had to deal with more than 50 incidents. The Association of Certified Fraud Examiners' (ACFE) 2002 survey found that, while companies of all sizes experience fraud, smaller companies suffer proportionately larger losses. And the ACFE estimated fraud losses in the U.S. at $600 billion in 2002, or 6% of revenues. Because not all incidents of fraud are detected and not all detected cases are reported, any fraud statistic is an estimate. The statistics make it clear that fraud occurs frequently, and no organization is immune.

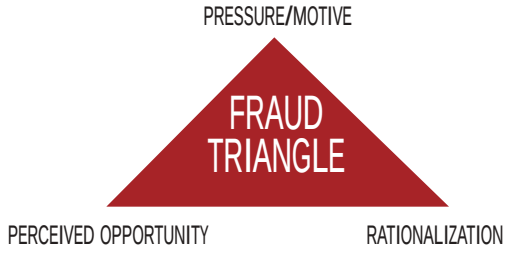
2. Anyone can commit fraud.

Researchers have failed to discover unique demographic characteristics of fraud perpetrators. Quite the contrary, fraud perpetrators are likely to be married, educated beyond high school, have an employment record of one to more than 20 years, range in age from their teens to their 60s or beyond, have no arrest record, are socially conforming, and are likely to belong to a church. In other words, their profile differs very little from the average person. The person likely to commit your company's next fraud could be sitting in the office right next to yours because, under the right set of circumstances, anyone could become a fraud perpetrator.

3. Why people commit fraud.

So what are the circumstances that encourage this kind of criminality? The best theory researchers have developed involves what's called the fraud triangle.

Specifically, three elements must be present in order for someone to commit fraud. First, there must be the motive or pressure to commit the fraud. This element is usually in the form of a real or perceived financial need,



but it can also take other forms, such as the desire to get even with the employer. Second, the perceived opportunity to be able to commit the fraud and get away with it must be present. Here, weak or missing internal controls often are enabling factors. The third element is rationalization, or the ability of perpetrators to find a morally acceptable excuse that justifies why their actions aren't a crime. Common rationalizations include: "I'm only borrowing the money and will return it as soon as I can"; "This company would fall apart without me, so I deserve this, and I'm not taking any more than is rightfully mine"; "Nobody is getting hurt"; "People would understand if they knew how much I need this"; or "Everybody does it." The good news is that a company can reduce the risk of fraud by eliminating any one component of the triangle.

4. The best deterrent is to increase the perception of detection.

So how does a company eliminate one of the triangle's elements? Note the key word "perceived" with the second item of the fraud triangle, "opportunity." Employees are much less likely to commit fraud if they believe they will be caught. Controls might be in place to detect a fraud in a timely manner, but if the employee is unaware of those controls, the fraud might still be committed. This principle also works in reverse—if controls are so deficient that anyone could get away with a fraud, but the employee believes that adequate controls are in place, the fraud will be prevented. Thus, the key to fraud prevention is to increase the perception that perpetrators will be caught if they commit one. This goal can be accomplished through any combination of the following: a strong system of internal controls, an obvious presence of internal auditors, fraud assessment questioning of employees, establishment of an anonymous hotline, and company-wide training to recognize the warning signs of fraud. Additionally, management should consider publicizing the results of fraud investigations to demonstrate to

employees that fraudulent activities won't be tolerated and will result in termination.

5. Perpetrators are often trusted employees.

Shock and disbelief are common reactions among coworkers when a colleague is charged with fraud. To be able to commit fraud, the perpetrator must have been in a position of trust. If an employee isn't trusted, controls are usually in place to monitor their job responsibilities, and the perception of detection is present. But many employers misplace trust in employees and often fail to implement the proper controls to reduce the risk of fraud. "I never thought Chris would do something like that" is a typical response by managers once they're informed that a fraud was committed by one of their employees. Blind trust is *not* an internal control.

6. Fraud schemes are not unlimited in number.

You can obtain a better understanding of the basic fraud schemes, how they are perpetrated, the common warning signs, and how they are prevented without obtaining professional certification in the fraud field. By far, asset misappropriation (or employee fraud) is the most common category of fraud. For example, the 2002 ACFE survey found that asset misappropriations comprised nearly 86% of the frauds studied, while the 2003 PwC international economic crimes survey reported 60% of respondents experienced asset misappropriation (product piracy came in a distant second at 19%). KPMG's 2003 fraud survey said 60% of respondents experienced employee fraud during the previous 12 months, with consumer fraud coming in second at 32%.

Asset misappropriation schemes usually focus on two categories of assets: cash and inventory. Cash, for obvious reasons, is the preferred asset of fraudsters, and the 2002 ACFE survey found that cash was the stolen asset 90% of the time.

So how do fraud perpetrators get their hands on the cash? It doesn't take a criminal mastermind to concoct two of the basic methods: (1) Steal the cash either before or after it's been recorded on the books (skimming or larceny, respectively), or (2) trick the employer into paying

Figure 1: Asset Misappropriation Schemes

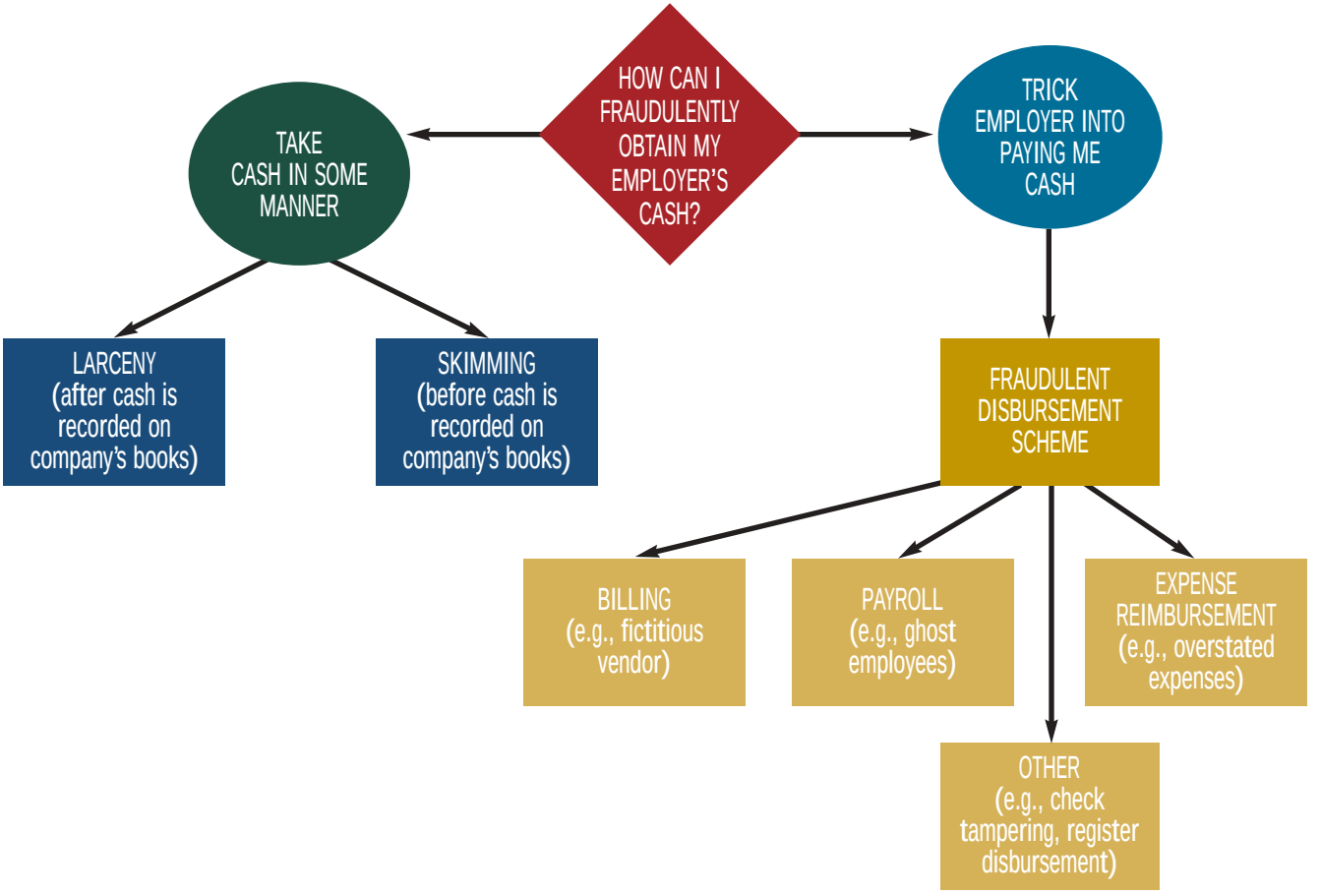
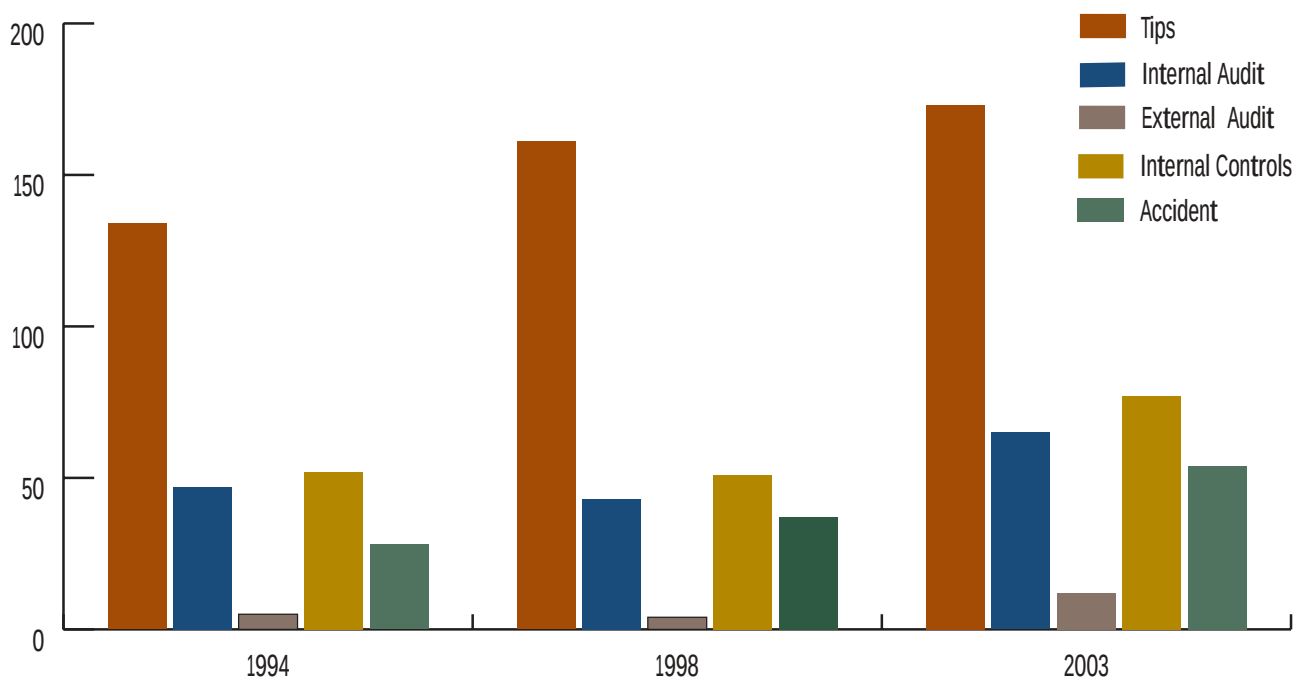


Figure 2: Methods for Discovering Fraud (KPMG's Fraud Surveys)



The percentage totals are greater than 100% because many respondents experienced more than one fraud. Tips include anonymous tips and notification by an employee, a customer, a vendor, or a regulatory or law-enforcement agency.

you the cash, say by perpetrating a fictitious vendor scheme (fraudulent disbursements). A fictitious vendor scheme is a billing scheme in which the victim organization pays invoices for which no goods or services were received, with the perpetrator controlling the shell company that bills the victim organization. Fraudulent disbursements can use schemes involving payroll, expense reimbursements, check tampering, or register disbursements. The method used by the perpetrator will depend on the controls in place (see Figure 1).

The various schemes are surprisingly simple. If you want to learn more about any particular type, there are many articles, self-study continuing professional education products, and books available describing these different ploys.

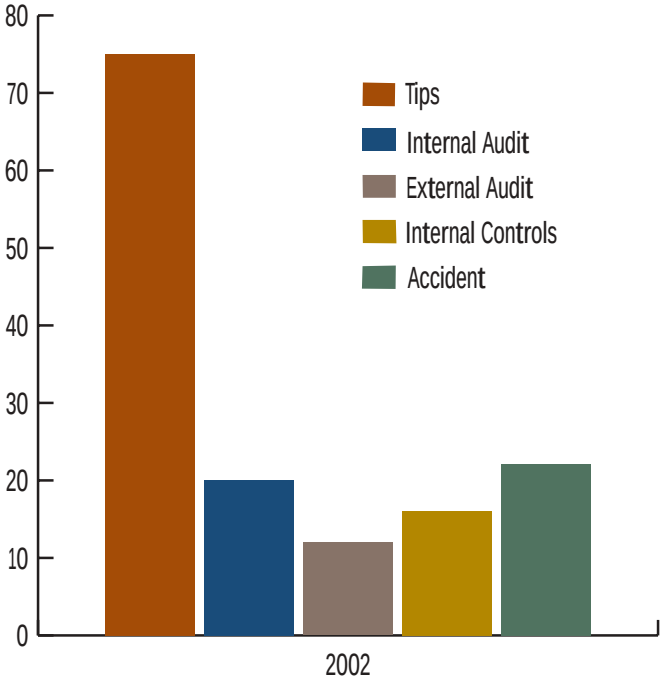
7. Red flags are only warnings.

No defense is perfect, so you want to be sure to understand how to detect fraud if it does occur. Knowing the red flags or warning signs is a good way to start. But it's important to remember that red flags are merely indicators of potential fraud—they don't automatically mean that fraud is occurring. Once you notice the red flags, you can begin an investigation into whether there are internal control weaknesses present and whether these weaknesses are being exploited.

Red flags can vary depending upon the fraud scheme. For example, invoices that are numbered consecutively (suggesting your company is the vendor's only customer), invoices that lack normal fold marks (suggesting it wasn't mailed), missing normal vendor information (such as a physical location or a phone number), or even-dollar amounts are some of the warning signs of a fictitious vendor scheme.

Virtually all fraud perpetrators spend most of their ill-gotten gains rather than saving the money, so when an employee starts showing signs of a lifestyle more extravagant than what his or her salary can legitimately support, it's time to start looking more closely at that employee's job responsibilities and the controls in place. KPMG's

Figure 3: Methods for Discovering Fraud (ACFE's 2002 Fraud Survey)



The percentage totals are greater than 100% because some respondents reported more than one method of discovering the frauds. Tips include anonymous tips and tips from an employee, a customer, a vendor, or notification from a law-enforcement agency.

1994 fraud survey reported that 48% of respondents indicated that there were red flags present with their discovered frauds, but they were either ignored or not acted upon quickly enough. The firm's 1998 survey found that the leading employee red flags were personal financial pressures (66%); abuse of drugs, alcohol, or gambling (48%); and extravagant purchases or lifestyle (42%). Ideally, both management and employees will be trained to recognize the red flags of fraud.

8. Auditors can't be relied upon to detect fraud.

Auditors rendering an opinion on your company's financial statements have a responsibility, according to professional standards, to provide reasonable assurance of detecting material misstatement, whether due to errors or fraud. In other words, auditors have no responsibility to detect immaterial fraud, and they provide no guarantee that all cases of material fraud will be detected. As we said earlier, most fraud cases take the form of asset misappropriation, and, undoubtedly, these schemes present an immaterial effect on the financial statements of large companies.

On the other hand, smaller companies can be materially affected by asset misappropriation schemes. PwC's 2003 survey found that detection by internal or external auditors was the most frequent means of detecting fraud (47%), with accidental discovery being second (32%), followed by tips (27%). But this finding is inconsistent with other surveys. For example, KPMG's surveys found that tips revealed frauds far more often than internal or external auditors. In addition, accidental discovery occurred more frequently than discovery by external auditors, and it came close to helping to detect frauds as often as internal auditors (see Figure 2).

Similarly, the ACFE 2002 survey found that the most common method of detecting fraud was tips from an employee (26%), with accidental discovery occurring more often than discovery by external or internal auditors (see Figure 3).

Despite PwC's findings, the firm states that it's worrisome for smaller companies to rely on an annual audit because that suggests they are placing too little attention on the development of effective controls and proper checks and balance. PwC warns that such overreliance may be playing into the fraudster's hands.

9. Hotlines and fraud assessment questioning are useful techniques.

Tips are a frequent means of discovering fraud, so how can you encourage them? Fraud assessment questioning (FAQ) and hotlines are two methods worth considering. (See sidebar on next page.)

Most employees are willing to reveal fraud if they are asked the right questions. FAQ is an interview technique that asks nonaccusatory questions designed to gather information about potential fraud, uncover internal control weaknesses, and identify other individuals possibly at risk for committing fraud. An additional benefit is that FAQ increases the perception of detection (discussed earlier) as fraud perpetrators find out that co-workers will be periodically asked to participate in these interviews.

Hotlines are also a useful technique. The 2002 ACFE survey found that companies with hotlines suffered median fraud losses of $77,500, compared to median losses of $150,000 for companies without hotlines. The survey reports that tips are a frequent means of detecting fraud, so providing employees and others with a way to report their suspicions makes sense.

Ideally, hotlines will allow for anonymous reporting.

There is still some stigma in our society attached to snitching, but, also, there will be very few employees willing to report their boss's fraudulent activities without the condition of anonymity. Hotlines should be available 24 hours a day because most employees will be reluctant to call during business hours when a colleague might overhear the conversation. Further, since the fraud perpetrator may be anyone within the organization, a third-party provider with properly trained professionals should operate the hotline. Finally, the company needs to adequately inform employees of the existence of the hotline and when they should take advantage of it. Employee training sessions, as well as posters and prominently displayed brochures, can help. Again, an added benefit of the hotline is the increase in the perception of detection.

10. Prevention is superior to detection.

The old proverb that an ounce of prevention is worth a pound of cure holds true with fraud. Fraud surveys indicate that the cost of fraud is staggering, and small businesses are less likely to be able to absorb a fraud loss and survive. KPMG's 2003 fraud survey reports the annual average cost of employee fraud to be $464,000, while PwC's 2003 survey finds the average loss because of asset misappropriation to be $1,388,731. The ACFE 2002 survey indicates that smaller organizations (with fewer than 1,000 employees) suffer significantly larger fraud losses than larger organizations. Fraud losses directly impact a business's bottom line, not the gross revenue. Thus, depending on the company's profit margin, for every $1 embezzled it will have to generate many times that in additional revenue to compensate for the fraud loss.

But fraud impacts more than just the bottom line of a business. Besides the dollar loss and cost of an investigation and prosecution, other nonquantifiable consequences of fraud can include low employee morale, loss of productivity, bad publicity, and loss of customer goodwill and future business. Because these costs are impossible to measure, their true impact will never be known.

A Matter of Paying Attention

Fraud is a crime, and, like all crimes, it doesn't happen only to other people. Further, it isn't something for just the accountants to deal with. As the fraud triangle illustrates, fraud prevention should be the responsibility of the entire company. Strong controls are needed to reduce the perceived opportunity for fraud. Providing proactive measures to detect fraud, through methods such as fraud assessment questioning and anonymous hotlines, gives employees the chance to help stop a fraud and, at the same time, increase the perception of detection, thereby preventing possible future frauds. This, in turn, can help to create a positive work environment that increases employee morale and reduces the pressure or motives to commit fraud. And the employee empowerment can lessen people's ability to rationalize their behavior if they feel that their actions impact the performance of the company and won't be tolerated by their co-workers. ■

FOR ADDITIONAL INFORMATION ON FRAUD ASSESSMENT QUESTIONING OR HOTLINES

- "Using Fraud Assessment Questioning to Detect Fraud," by Thomas A. Buckhoff and James D. Hansen, *The CPA Journal*, April 2001, pp. 36–40.
- "To Catch a Thief," by James D. Hansen and Thomas A. Buckhoff, *Journal of Accountancy*, March 2000, pp. 43–46.
- "The Benefits of a Fraud Hotline," by Thomas A. Buckhoff, *The CPA Journal*, July 2003, p. 62–63.
- For more information about a three-day "problem-based boot camp" on fraud investigations, initiated in 2004, see http://www.fraud-wise.com/training.htm.

NOTE: All of the above articles can be accessed online. See: http://www.nysscpa.org/cpajournal/2001/0400/features/f043601.htm, http://www.aicpa.org/pubs/jofa/mar2000/hansen.htm, or http://www.nysscpa.org/cpajournal/2003/0703/dept/d076203.htm.

Bonita K. Peterson, CPA, CMA, CIA, Ph.D., is an associate professor of accounting at the College of Business, Montana State University, Bozeman, Mont. You can reach Bonita at (406) 994-4620 or bonitap@montana.edu.

Paul E. Zikmund, CrFA, CFE, is director of Forensic Audit at Tyco International, Inc., Princeton, N.J. You can reach him at (609) 720-4415 or pzikmund@tyco.com.