Fraud: Discovery and Action

Don't learn the hard way!

By Ronald Cote

Small organizations sometimes assume they're immune to fraud. But the truth is that small organizations are the most vulnerable to fraud and financial abuse. Average loss to a small organization is $127,500 per incident, while a large organization's average loss is $97,000 per incident.[1]

The most common way of detecting fraud is through a tip from employees. The second most common detection method is "by accident." Don't wait till you accidentally discover fraud in your organization.

Besides Yelling "Fraud," What Do We Do?

When you first suspect fraud, your response should arise from your organization's written contingency plan. Be sure you prepare this plan well before fraud occurs and review it at least annually for possible update. The plan's creation should be a collaboration to address the needs of your organization's CEO, CFO, board, audit committee, general counsel, internal audit department, and senior staff.

Your contingency plan should lay out the steps to take when you discover fraud, including how you will investigate. The objectives of your investigation will depend on your unique circumstances, including the fraud's type and duration, number of perpetrators, and the rank of those involved. Monetary restitution is the most common form of relief sought. You and your organization's lawyer may wish to create a legal document stating that the perpetrator will repay what was taken. If an adversarial relationship develops, you may need to use civil remedies, such as mediation, arbitration, or trial.

If your objectives include punishment, you'll need to contact a law enforcement agency such as state and local police, the FBI, or the IRS, and attract a prosecutor's interest.[2] Enforcement officials and prosecutors may undertake their own analysis to determine the benefit of pursuing your case.

Preventing fraud (or detecting it shortly after initiation of a scheme) will be more cost-effective and less

continued on page 22

Glossary

Asset Misappropriation: Theft of tangible assets by an employee. Asset misappropriation schemes include lapping receivables, pilfering inventory, creating ghost employees, and redirecting customer payments to an unauthorized account or recipient. Damage can manifest itself in the form of decreased customer service, improper billings, increased prices, default on debt, and even bankruptcy.

Assets: Things of value that can be measured and expressed in money terms.

FASB (Financial Accounting Standards Board): Accounting organization that sets external accounting procedures for nonprofit organizations.

Fraud: Intentional perversion of truth to induce others to part with valuables or to surrender a legal right. Forensic accountants categorize fraud as: 1) asset misappropriation committed by employees; 2) financial statement manipulation committed by employees; 3) asset misappropriation as a result of collusion between employees and outside vendors or customers; 4) theft of trade secrets or intellectual property by a former employee or competitor; or 5) bribery between an employee and a government official.

Fraudulent statements: Assertions made to deceive someone into relying on documents which have been falsified in terms of an organization's operational, financial, or market performance.

GAAP (Generally Accepted Accounting Principles): Standard methods which organizations must follow in presenting their financial information. For nonprofits, these standards are set by the FASB.

> The most common method of detecting fraud is through a tip from employees.

disruptive than investigating a well-established fraud scheme. Effective fraud prevention requires creating an internal control system and monitoring it proactively (see Sopher in "Resources").

Understanding your organization's unique risks is the starting point to designing effective controls. For example, weak "segregation of duties" is a common control problem. Ask yourself questions such as the following to assess your risk:

• **Do you segregate duties** in the accounts payable function?

• **Do you make sure** the disbursement process complies with organizational policy?

• **Do you restrict** the amounts that one person can disburse without a second signature?

• **Are costs** monitored closely?

• **Does the disbursement system** allow for manual checks?

• **Are canceled checks** (or the like) returned from the bank?

If you can't answer "yes" to these questions, consider making changes to lessen your risk.

Organizational Impact of Fraud

• **On average, an organization** will lose 6% of its annual revenues to internal fraud.

• **The average length** of a fraudulent scheme is 18 months.

• **Schemes involving non-cash assets** are more costly than schemes involving cash. The median loss for cash

Recognize the Red Flags

The Most Common Fraud: Misappropriation

The great majority of occupational fraud (80%) involves asset misappropriations. Of those, 90% involve cash as the target asset. The median loss for cash theft is $80,000, while the median loss for non-cash misappropriations is $200,000. Watch for these signs of misappropriation:

- **a decreasing ratio** of cash to total current assets or ratio of cash to credit card sales
- **flat or declining sales** that occur while the costs of sales increase
- **increasing accounts receivable** compared to cash
- **delayed posting** of accounts receivable payments
- **unexplained discrepancies** in cash sheets or bank reconciliations
- **altered** deposit slips
- **customer** billing and payment complaints
- **increasing "soft" expenses** (like "consulting," "temporary labor," and "advertising")
- **an employee's home address** that matches a vendor's address
- **a vendor address** that is a post office box
- **a vendor name** that consists of initials
- **a vendor** with a vague business purpose
- **excessive "void," missing, or destroyed checks** (particularly if manual checks or new check stock is used)
- **pre-signed** checks
- **unsecured** signature plates
- **lack** of account reconciliations
- **employees who seem to be living** beyond their means
- **employees who never** take vacations
- **family members** of the CEO or key senior executives who are employed by the organization
- **a weak** internal control environment.

The Fraud that Concerns Auditors Most: Financial Misstatements

Auditors are constantly alert to cases of financial misstatements because such misstatements always violate one or more of the eight major GAAP standards.* Signals that an organization may be manipulating its financial statements include the following:

- **Executives of the organization** lie to auditors or ask "why" the auditor seeks certain information.
- **The organization tends to be dominated** by one person or a small circle who act in unison.
- **Managers argue** with auditors about the aggressive application of accounting principles.
- **The organization often reports financial results** "at the last minute" or late.
- **A large portion of management compensation** depends on meeting quantified targets.
- **The organization is in a period** of rapid growth.
- **There are consistently increasing "deposits in transit" amounts** on bank reconciliations.
- **The organization has large "one-time" expenses** that reportedly don't affect operating results.
- **There is a long-tenured controller** with strong centralized control.
- **Obsolete inventory** is priced at current levels.
- **The organization always meets** revenue projections.
- **Multiple related-party relationships exist** between the organization and its vendors, suppliers, or customers.

*These eight standards are: materiality, matching, conservatism, going concern, cost, objective evidence, consistency, and full disclosure. Common schemes related to financial misstatements include "cookie jar" reserves, revenue smoothing, early recognition of revenue, fictitious revenue, deferral of expenses, reorganization costs and other "one-time" charges, manipulated capitalization periods for fixed assets, "off book" risks, over-valued assets, misreported contingent liabilities, misclassified investments, and manipulation of performance indicators.

Prevention and detection cost much less than correcting fraud after the fact.

theft is $80,000, while the median loss for non-cash misappropriations is $200,000.

• **The typical perpetrator** is a first-time offender.

• **As perpetrators get older**, their schemes become more costly.

• **Men out-steal women** $200,000 to $60,000 per incident.

• **People with bachelor degrees** take more ($243,000) than those with high school educations ($70,000) or those with post-graduate degrees ($162,000).

These costs spiral outward and multiply at a terrifying rate as we examine the costs of fraud to insurers, lenders, our justice system, and the nonprofit sector as a whole.

Small organizations are the most vulnerable to fraud and abuse.

The Fraud Fight Is Forever

The value of a fraud prevented is difficult to quantify. After such an event takes place, it's clear that prevention and detection cost much less than correcting fraud after the fact.

There will always be people willing to take advantage of others' trust and gaps in controls. But as awareness grows, and professional watchdogs sharpen their senses, you can reduce your exposure to fraud and respond with an organized plan if you're ever faced with a fraudulent employee. ■

Footnotes

[1]These and other figures in this article come from the Association of Certified Fraud Examiners' "Report to the Nation: Occupational Fraud and Abuse."

[2]From *Fraud Auditing and Forensic Accounting: New Tools and Techniques* by G. Jack Bologna and Robert J. Lindquist.

Resources

Messina, Frank M., "Common-Sense Approaches to Fraud Awareness, Prevention, and Detection," *Nonprofit World,* Vol. 15, No. 4.

Ross, Frank, "The Audit Committee: Why You Need One, How to Form One," *Nonprofit World,* Vol. 6, No. 6.

Sopher, Marti, "Setting Up a Control System for Your Organization," *Nonprofit World,* Vol. 16, No. 3.

These resources are available at www.snpo.org/members.

Ronald Cote, CPA, CFE (Ronald.Cote@gt.com), is senior manager with Grant Thornton's Chicago Forensic Accounting & Investigative Services practice. He has over 15 years' experience in accounting. This article is excerpted from his presentation to the Michigan CPA Society.