

White Collar Crime

Identifying, Responding to and Investigating Internal Fraud

By Alan C. Winters and
Michael J. Molder

While newspapers headline larger scale corporate fraud like R. Allen Stanford, Madoff, Tyco, etc., fraud often occurs in small and medium-sized businesses like ours and our clients'. A common type of fraud is defalcation or misappropriation of assets. A defalcation can involve a misappropriation of cash, supplies, inventory or other business property.

Defalcation is most often committed by employees who have a close relationship with the owner/operator and wear multiple hats within the company

Winters is a partner in the forensics and marital dissolution practice groups at Marcum LLP, a large independent public accounting and advisory firm. He is often appointed by the court system as a fiscal agent, provisional director and custodian and is on the roster of selected mediators for economic aspects of N.J. family law cases. Molder specializes in litigation support services in the firm's advisory and forensics practices groups. His experience includes pending or threatened litigation as well as internal investigations of financial misconduct.

or practice, i.e., accounts payable, payroll, accounts receivable and bookkeeper. Lack of segregation of duties, along with other inadequate internal controls, creates opportunities for fraud. In larger organizations, perpetrators tend to be the individuals with some degree of management authority: CFO, controller or accounts payable/receivable manager.

In each case, fraud requires access and knowledge. To counter internal fraud, management should be very familiar with all of the following: signs of potential fraud; considerations when responding to a fraud scheme; and how to investigate potential subjects of a misappropriation.

Signs of Potential Internal Fraud

Time is of the essence — the earlier fraud is detected, the better! Unfortunately, in many cases it is only when the fraudster makes a mistake, becomes lackadaisical or the business declines that fraud is discovered. By then, loss and reputational damage are often already significant. Management vigilance is essential.

According to the Association of Certified Fraud Examiners, employees discovered engaging in fraud generally are:

- males between ages of 31 and 45;
- college educated;

- controlling and unwilling to share responsibilities;
- extremely trusted and perform multiple roles within the business;
- unlikely to take their full allotment of vacation time for many years in a row;
- in financial difficulty and/or living beyond their means;
- suffering from problems with drugs, alcohol or gambling; and/or
- guarded and unwilling to allow review of their work product.

Note: these characteristics do not definitively determine that an employee is involved in a fraudulent act. Rather, they are signals that a problem may exist, or could develop, and warrant investigation.

Internal Controls Are Every Business's Best Defense

Internal controls, like every other aspect of running a business, incur costs, but, as with most other things, being "pennywise" may lead to being "pound foolish." Additionally, establishing an effective control environment is a fraud deterrent in itself — the prospect of discovery can reduce the occurrence of fraudulent behavior.

Segregation of duties involving cash receipts and disbursements is a critical

internal control that no organization should overlook. The same individual should not approve, process and reconcile cash transactions. Controls must exist over the maintenance of vendor and employee lists, particularly new entries, to decrease the opportunity to create fictitious payees. Restricting and monitoring user access to the accounting systems, via passwords and user activity logs, is an important control that should be in place in every organization.

Simple procedures can be performed to prevent the potential misappropriation of an asset. Receipts are best opened and immediately endorsed with a stamp stating "for deposit only" by someone *other than* the individual who prepares the deposit. Cash and checks should be kept in a locked and secure area until they can be deposited.

Management must actively participate in the control environment:

- Review copies of cash disbursement journals or actual checks and bank reconciliations on a regular basis — no less frequently than biweekly.
- Review vendor lists at least monthly and require management authorization for new vendors.
- Investigate *all* unusual variances in business activity.

These procedures not only reveal potential asset misappropriation schemes, but they also establish management's active participation in the control environment.

Considerations for Response to a Potential Fraud Scheme

If fraud is suspected, the first consideration is whether to handle the issue internally or pursue criminal sanctions. Involving police or a prosecutor risks management's control of the investigation. As one of many cases the authorities are investigating, yours may not be a high priority.

Thus, business owners must evaluate the salient facts and their ultimate objectives regarding potential restitution and punishment. This is not a simple decision as investigations (whether internal or external) can be time-consuming and expensive, and the likelihood of recovering the misappropriated funds or property may be remote. Consultation with counsel and forensic

accountants can be essential to effectively evaluating options.

Forensic accountants investigate, analyze, interpret, summarize and present complex financial information. The work of forensic accountants and/or damages experts includes quantifying the extent of the company's loss due to a fraud; gathering evidence of how the fraud was perpetrated; and suggesting how fraud can be prevented in the future

Conducting an Investigation

If opting for an internal investigation, the investigator must conduct it in a way that builds credibility with the company's personnel as well as outside regulators, customers and, possibly, the media. Experienced counsel and fraud investigators should be retained as soon as possible to ensure that any investigative procedures meet the specifications of the law and documentation is properly preserved.

A decision should be made as soon as possible regarding who will be responsible for the investigation — i.e., the business owner or manager, audit committee, internal audit department, board of directors, outside counsel, forensic accountant or a combination of these. This decision should be based on factors such as the size of the potential fraud, the targets of the investigation, the ability to recapture stolen funds and the overall risk to the company. The designated leaders should outline the scope of the investigation, establish a preliminary list of employees, vendors, and/or customers to interview, and designate documents and data for review.

The responsible person should also outline preservation guidelines for evidence, including electronically stored information. Given that documentary evidence is the keystone to most civil litigations, it is important to address this issue early on in the investigation. To this end, employees should be alerted to preserve relevant data. The investigator must also evaluate the need for qualified computer forensics and data preservation experts. Computer forensics experts can help find hidden or hard-to-find data and recreate critical deleted data and other computer-related events. A firm experienced in using computer forensics will also ensure the

integrity of the evidentiary chain of custody.

Conducting an Interview

The interview process is, in many respects, an art form. It is a complex process that can take many shapes depending on the scope of a particular investigation. The process requires highly qualified and experienced investigators to control the questioning and capture the witness's responses, as well as visual and sensory cues regarding the witness's body language and vocal inflections.

The investigator must develop an overall interview strategy and targeted list of topics. However, the interviewer must also be flexible, keeping in mind that no two interviews will be the same. It is difficult to know if someone is involved in the fraud until you begin your investigation. One interviewee may want to tell you what they have done, while another will not tell you anything and is only looking to find out what you know. The interviewer has to have the ability to gain quality information and cause the interviewee to respond, in order to detect deception. The interviewer also needs to keep in mind that once the investigation and interview process has begun, you may have only one chance to interview a person. For these reasons, it is essential for management to engage an experienced professional with years of experience interviewing witnesses regarding employee theft in large and small businesses, involving company funds, inventory and other types of assets and interests.

Best practices dictate that management should maintain established internal control policies and procedures, such as segregation of duties and regular evaluation of the effectiveness of all preventive measures that are in place. If an internal control environment does not exist, management is gambling that employees will behave ethically which, unfortunately, is not always the case.

Business owners and operators should also monitor for the early warning signs to aid in the detection of employee fraud and, if they come to suspect fraud, should only proceed with highly qualified professionals. ■