Reprinted from
The Journal of Corporate Renewal

How Private Companies Can Prevent Fraud

Irregularities Jump-Start Probe at Battery Manufacturer

By John D. Connor, CTP, CFE, Principal,
Anderson Bauman Tourtellot Vos & Co.

Fraud is a major problem for Corporate America. More than 70 percent of U.S. corporations reported some form of fraud over the past three years. On average, an American company loses almost 5 percent of its revenue to fraud every year at an annual cost to the U.S. economy of $650 billion. Despite this huge toll, only one in three corporations has implemented effective fraud prevention measures.

Privately held companies are beset by financial statement fraud, asset misappropriation, bribery and corruption, and theft of intellectual property. To prevent these behaviors, it is helpful to understand the causes. Occupational fraud occurs when there exists situational pressure, an ability to rationalize unacceptable conduct, and a perceived opportunity to commit the crime.

Individuals will always be subject to situational pressures, such as oppressive debt, mounting medical bills, or expensive addictions. Fraudsters typically rationalize their behavior with thoughts such as, "I'm just borrowing the money." When high pressure is coupled with rationalization, people may be tempted to test the opportunities to steal.

Companies can't do much about the personal pressures their employees are subjected to, and there is a limit to how much they can influence honesty. But there are strong measures they can implement to prevent and deter occupational fraud.

The following case illustrates how fraud can occur and how effective measures could have been instituted beforehand to remove the opportunities for fraudulent activities.

An automotive battery manufacturer had two manufacturing plants and 12 remote distribution centers. Each plant and distribution center collected used batteries amounting to one used battery for each new battery sold. The used units were graded as either recoverable or nonrecoverable. Recoverable units were cleaned, recharged, and sold through independent service stations around the plants and distribution centers.

Refurbished units usually were sold for cash paid directly to the delivery truck drivers, who were responsible for recording sales and returning cash to the administrative staff at the plant or distribution center. Further, each remote distribution center maintained an imprest petty cash fund of $5,000. Finally, the national sales manager, "Fred," was responsible for operation of the distribution centers.

> Occupational fraud occurs when there exists situational pressure, an ability to rationalize unacceptable conduct, and a perceived opportunity to commit the crime.

Fred lived in a small town in Ohio, where one of the distribution centers was located. His two sons worked at the distribution center, as did Fred's best friend, "Barney," who was the distribution center manager and reported directly to Fred. Barney was responsible for the employees who graded the recoverability of the batteries.

Back at corporate headquarters, the distribution department noticed increases in the percentage of used batteries that were being graded as nonrecoverable, which it found difficult to explain. A study across all plants and distribution centers revealed that dramatic changes in the recovering rate had occurred at the Ohio distribution center over 18 months. While the nonrecoverable rate at all other distribution centers averaged 60 percent, the Ohio center showed a 90 percent nonrecoverable rate.

The company began an on-site investigation and soon heard from lower-level employees that Fred's sons had been seen loading returned batteries into a pickup truck after hours and on weekends. The investigator also found that the recoverability grade documents had been altered prior to entering the data into the computer system.

Finally, a disgruntled employee came forward and told of apparent collusion among Barney, Fred, and Fred's sons to refurbish batteries and sell them to regional independent dealers for $10 each. This group also routinely took new batteries from stock and prepared documents that graded them as non-recoverable. The new batteries were then sold at full price to the independents. All transactions were in cash but were seldom fully recorded on the company's books.

It was later proved that the cash, which totaled $1.8 million, had been pocketed by Fred and his cohorts. The perpetrators were dismissed immediately, but no criminal charges were filed and no civil action was brought. A small settlement was received from the company's insurance carrier under the employee dishonesty rider.

Sending the Right Message

In this case, executives at corporate headquarters weren't paying enough attention to what was going on in their distribution network, nor had they implemented basic policies and measures to signal to employees that theft was completely unacceptable and would result in swift and severe penalties.

Here are nine anti-fraud measures that could have saved this company $1.8 million and should be standard policy at privately held companies:

1. Institute an Employee Hotline. Employees need a channel through which they can report information anonymously, as they might well have done at the battery company, where lower-level employees were aware of suspicious activity. The phone number employees can use to leave a recorded message should be posted on bulletin boards and published in the employee handbook.

Providing this channel is important because employees are often intimidated by perpetrators of workplace crime and fear that financial or physical harm will come to them if they report wrongdoing. A hotline can be a deterrent, too. Those tempted to steal may

▶ See page 2

PREVENTING FRAUD, from page 1

think twice about it when they know they risk being seen and reported.

2. Set a Principled Tone at the Top. At the battery company, the owners and top managers shared virtually nothing of their vision for the organization. Since they didn't communicate, their employees tended to think that nobody was watching them. To deter fraud, leaders should make ethical standards part of the vision and mission statements for the business and make sure that those statements are posted and published where all can see them regularly.

3. Develop a Code of Conduct. Beyond a general statement of ethics, companies need a written code of conduct, with penalties for violations clearly stated. Employees should be required to read and sign a document stating that they agree to abide by the code. The company also must live by the code, following through with dismissals, civil lawsuits, or criminal prosecution, no matter how high-level the perpetrators of fraud. At the battery company, nobody had even thought about the penalties for fraud or considered that all new employees should be informed of the expected code of conduct.

4. Hire and Promote Appropriate Employees. The Freds of this world frequently are charming and affable. No matter how smooth and plausible a candidate may appear, smart companies conduct background checks and obtain credit ratings. References from previous employers aren't enough, as they are constrained in what information they can reveal and are subjective at best. For objective data, check public records for criminal convictions and get a candidate's permission to perform a credit check.

5. Institute Continuous Training and Communications. The executives with the battery company didn't get out much. By not communicating frequently with employees at the distribution centers and never visiting them, they set the stage for opportunities to steal. Companies should set up mechanisms and channels whereby employees are aware of management and understand the expectations of upper management.

6. Administer Fair and Balanced Discipline. To work as a deterrent, policies regarding misbehavior must be enforced evenhandedly across the board. Whether the penalty is "three strikes and you're out," instant dismissal, or criminal prosecution, companies are better off risking whatever negative publicity may come about as a result of punishing infractions than ignoring or concealing them. Intolerance of unethical behavior must be unwavering and consistent to create an environment that truly discourages fraud.

> Those tempted to steal may think twice about it when they know they risk being seen and reported.

7. Identify and Monitor Fraud Risks. Occupational fraud is the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets. Simply put, fraud is the theft of assets, and companies need to look at the controls over all of their assets.

The battery company's leaders had never thought to have their accounting firm look at their distribution centers as places where the company might be exposed to fraud, though clearly the recordkeeping controls at the warehouses were not tight enough. Companies are well-advised to have their accountants identify areas in which fraud could occur, implement more controls as recommended, and then do follow-ups as needed to ensure that the new controls are working.

8. Implement and Monitor Internal Controls. At the battery company, transactions at the remote warehouses were done on a cash basis. Drivers took the money to Fred, who passed it along to a clerk, who deposited it in the bank. With this process, it was easy for Fred to pocket some of the cash. Companies need to look carefully at their processes and at splitting duties among employees, so that the individual who receives payments, for example, is not the same person who records deposits and reconciles the books.

9. Work with an Independent External Auditor if Fraud Is Suspected. It took some outside expert assistance to crack *The Case of the (Allegedly) Dead Battery,* and that is par for the course. It's a rare company that has someone in-house with the skills, knowledge, and objectivity to investigate and prove fraud.

Insiders may have preconceived notions, which may make them less likely to suspect and question trusted employees — or they may be in on the fraud themselves. They may be blind to shortcomings in systems and practices that are virtual invitations to theivery.

Although a company's regular public accounting firm may be technically competent to investigate fraud, it may not be the best candidate for the job. Certified fraud examiners, often found in some turnaround management firms, forensic fraud firms, and some large CPA firms, typically are accountants who also have extensive experience in uncovering newer and less obvious forms of theft. The information technology area, for example, presents many opportunities for fraud that may slip though an annual audit. "Ghost" employees on the payroll are but one way to use technology for lucrative skimming.

Implementing some fairly simple, direct, low-cost anti-fraud measures can go far toward making a company a place where cheaters seldom prosper and honesty really is the best policy. •

John D. Connor, CTP, is a principal with Anderson Bauman Tourtellot Vos & Co., a turnaround management firm. Before joining the firm, he was active in the financial management of manufacturing operations and, as director of finance for a Fortune 500 company, implemented one of the first activity-based costing systems in the U.S. As a turnaround manager, he has served clients in more than 20 industries. Connor is a Certified Fraud Examiner.