GROSS MENDELSOHN

ACCOUNTING | TECHNOLOGY | WEALTH ADVISORY

How To Protect Your Business From Employee Fraud

BEST PRACTICES GUIDE

Understanding Who Commits Fraud And Why

There are three conditions that are generally present when fraud occurs:

1. The individual is experiencing pressure
2. The individual perceives there is an opportunity to commit fraud
3. The individual lacks personal integrity and rationalizes that committing fraud is justified

These three conditions — pressure, opportunity and rationalization — are referred to as the fraud triangle. All three factors are usually necessary for a fraud to occur.

Employees who commit fraud are usually motivated by pressure caused by financial problems, personal habits or work-related issues. Financial pressure could result from excessive debts, medical bills, overuse of credit cards, going through a divorce or investment losses.

Personal habits such as drug, alcohol or gambling addiction, extramarital affairs and living beyond one's means also create pressure.

Employees Who Commit Fraud Often Rationalize Their Acts

The personal integrity of most individuals keeps them from committing fraud. However, some employees rationalize their fraudulent acts.

They might convince themselves they are only borrowing the money and will pay it back, the money is being used for a good purpose, the losses are covered by insurance so the company will not be hurt by the losses, or have the mindset that "the company treats me unfairly and owes me."

Opportunities to commit fraud arise when internal controls (proper checks and balances) are weak or nonexistent.

Work-related issues could include the employee believing he or she is underpaid, unappreciated, not respected or treated poorly.

In most cases the employee who commits fraud is someone who is a "trusted" employee. Employees who have worked for a company for a long period of time usually gain more trust from their supervisors and coworkers and therefore their actions may not be closely monitored. Also, the dollar amount of fraud losses tends to increase based on the number of years the employee has worked for the company and the employee's level of authority within the company.

Fraud perpetrators typically do not have the characteristics usually associated with criminals. Most have no prior criminal record and no history of termination by a prior employer due to fraud. But, according to the Association of Certified Fraud Examiners' (ACFE) Report to the Nations, in 85% of fraud cases the fraudster displayed one or more behavioral "red flags" that are often associated with fraudulent conduct.

YOU MAY ALSO BE INTERESTED IN

A Texas-Sized Fraud: Bookkeeper Embezzles $29M From Texas Family

How to Prevent Fraud At Your Small Business

Fraudsters Love Lax Expense Reimbursement Policies

Typical Red Flags And Fraud Schemes

What Are Red Flags?

Red flags are clues that a fraud might be occurring.

Management should recognize behavioral red flags when they occur and take steps to investigate whether such clues lead to discovery of information that substantiates acts of fraud. However, be careful not to jump to conclusions based solely on the presence of a red flag.

Examples of behavioral red flags include:

- Living beyond means
- Financial difficulties
- Unusually close association with vendor/customer
- Unwilling to share duties, refuses to take time off
- Divorce/family problems
- "Wheeler-dealer" attitude
- Irritability, suspiciousness or defensiveness
- Bullying or intimidation
- Addiction problems

Employee Fraud Schemes To Watch For

While there are many types of employee fraud schemes, some of the more common types are:

- Creating fictitious vendors — dummy companies from which nonexistent services or materials are being purchased
- Check tampering — altering payee, altering amount, forging signature, forging endorsement
- Stealing supplies, tools and equipment
- Payroll — creating ghost employees, overstating hours worked
- Making personal purchases, abusing expense reimbursements
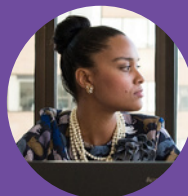
Article You May Be Interested In

How Too Much Trust Can Erode Internal Controls

Implementing Fraud Prevention Policies

Your management team should recognize that fraud can occur in any business, no matter the industry or size of the organization, and that almost any employee may be capable of committing fraud given the right set of circumstances. Therefore, management should maintain a heightened awareness of fraud and implement fraud prevention policies.

Creating a company culture that promotes honesty must begin with the "tone at the top," the example set by the conduct of owners and management. Employees who observe owners and management acting in an unethical manner will consider such behavior to be acceptable.

Businesses should establish anti-fraud policies, including communicating to employees how to report suspected fraud and assuring employees that the company encourages such reporting.

Honest employees are more likely to report fraud when the organization invites and encourages them to do so. According to the ACFE, the most common method of detecting fraud, by a wide margin, is through employee tips.

Management should maintain a heightened awareness of fraud and implement fraud prevention policies.

Employers cannot control an employee's financial pressures, personal integrity or rationalizations. But the employer can put controls and policies in place to limit the opportunities an employee has to commit fraud.

It is much easier to prevent fraud than it is to detect fraud. Increasing the perception that fraud will be discovered is the most effective fraud prevention method. Most employee fraudsters are first-time criminals and they are less likely to steal when they perceive there is a high probability they will be caught.

No system of internal controls can fully eliminate the risk of fraud, but well-designed and effective internal controls can deter the average fraudster by reducing the opportunity to commit the fraud. Effective internal control includes a company culture of honesty and integrity (tone at the top), an effective and secure information system, and appropriate control and monitoring activities.

There are a number of fraud prevention techniques that businesses should implement.

- Bank statements should be mailed directly to someone not involved in bank transactions (check writing, deposits, transfers, etc.), such as an owner, who should review the statements and cancelled checks
- Bank reconciliations should be performed timely, preferably by a trained employee not involved in bank transactions
- Segregating duties, such as the responsibility for authorizing transactions, recording transactions and maintaining custody of assets should be assigned to different employees
- Requiring periodic job rotation and mandatory vacations
- Requiring authorization and approval of transactions with appropriate dollar limits — check signing, purchase orders, credit cards, etc.
- Physical controls over documents and records — storing blank checks in locked cabinets, use of password protection of computer files
- Physical safeguards over assets — security measures, consider surveillance cameras to monitor materials, tools and equipment
- Implementing a whistleblower program
- Preparation of timely and detailed monthly financial statements closely reviewed by management

YOU MAY ALSO BE INTERESTED IN

[Tips For Preventing Disbursement Fraud In Your Business](#)

[Using Internal Controls To Protect Your Nonprofit Association From Fraud](#)

Why Fraud Controls Break Down

There are limits to what internal controls can do to prevent fraud. It is impossible to implement internal controls that eliminate the possibility of fraud. Breakdowns in internal controls can occur for a number of reasons, including collusion and override of controls by management.

Collusion is when individuals act collectively to perpetrate and conceal an action from detection. An individual in a management position may perpetrate a fraud by overriding controls and directing employees to deviate from the standard company policies and practices.

Controls can also break down if well-designed internal control policies and procedures are not followed because management team members place significant trust in an employee and therefore do not believe it is necessary to perform the checks and balances with respect to that employee's work.

Policies are designed and put in place for a reason and you should never deviate from company policies based on trust and a belief that an employee is not capable of committing fraud.

Why Have A Hotline For Reporting Fraud?

According to the ACFE, organizations with some sort of hotline in place saw a much higher likelihood that a fraud would be detected by a tip (46%) than organizations without a hotline (30%).

The presence of hotlines, formal management reviews and employee support programs were correlated with the greatest decreases in financial losses.

GROSS MENDELSOHN

ACCOUNTING | TECHNOLOGY | WEALTH ADVISORY

About The Author

Richard Wolf, CPA/ABV, CFE, CVA, is a partner at Gross Mendelsohn. He is the director of the firm's Forensic, Valuation & Litigation Support Group.

Richard enjoys the puzzle-like aspects of fraud investigation. He helps clients determine how a fraud was committed — and how the perpetrator concealed the fraud — by piecing together past actions. Richard knows how to pore through thousands of pages of documents to find the key evidence in a case. In addition to being a CPA, Richard is a Certified Fraud Examiner, a Certified Valuation Analyst and Accredited in Business Valuation.

Request A Consultation

Contact Us

410.685.5512

rwolf@gma-cpa.com

www.gma-cpa.com