

How to Battle Corporate Fraud and Balance Employer Security with Employee Privacy

By Joseph Centofanti, CPA, CFE, FCPA, CGFM, Kostin, Ruffkess & Company, LLC

Combating corporate fraud and striking a balance between employer security and employee privacy is no easy task, but it can be accomplished when an employer communicates its corporate culture through specific policies and procedures. That being said, these policies must clearly convey the expected behavior of employees. In short, the purpose of all company policies is to protect both the company and its employees in situations where it appears that something may have gone wrong.

Policies can address a variety of areas, including company property, data security, expectation of privacy, and even an employee's responsibilities for reporting to management known violations of the employer's policies and/or illegal acts. They can range from a general code of conduct or code of ethics policy to certain general personnel policies, addressing issues such as basic travel reimbursement or the employer's position on fraud and use of the company's IT resources.

Battling fraud and balancing employer security with employee privacy are key areas that warrant specific policies. Every employer should consider establishing and implementing these policies to strengthen its company culture, set the tone from the top and ensure that employees are acting in ways that do not put the company at risk.

Create a Fraud Policy

Although a significant number of employers have a code of ethics or code of conduct policy, these policies rarely address fraud specifically or in adequate detail. Therefore, every employer should have a separate fraud policy. This policy details clearly the employer's position regarding fraudulent activity, defines what is considered to be fraudulent activity and communicates the consequences to the employee if they are found to have engaged in any fraudulent activity.

A fraud policy also speaks to employees about their responsibility to identify and communicate to the appropriate level of management if they suspect or are aware of fraudulent activity. The policy is not meant to list all possible examples of occupational fraud but to provide information to employees that will clarify activities that may not always be viewed as fraud. Examples of these activities include such things as:

- a. putting time on a timesheet/card that the employee did not work,
- b. putting expenses on expense and travel reimbursements that are not for the proper amount or for company business, and
- c. use of company equipment and office supplies.

In addition, the policy should communicate zero tolerance for fraudulent activity along with the possible consequences, including immediate termination.

Finally, a fraud policy should be included in or with the employee personnel policies provided to a new employee. As with all personnel-related policies, the company should have a signed document from the employee stating they have received and read the company policies.

In general, employees have a duty to cooperate during an internal or other investigation as long as what is requested from them is reasonable. This duty varies state to state and is affected by statutory and common law.

Balance Employer Security with Employee Privacy

There are other employer policies that collectively are critical to avoid potential problems in the event of internal investigation or workplace search. All these policies have one thing in common, in that, they reduce the employee's expectation of privacy.

The expectation of privacy issue relates primarily to workplace searches. These expectations cannot be lowered to zero by policies but can be lowered to a significant degree. There is no bright line or safe harbor to determine if an employee has a reasonable expectation of privacy for a particular area. Some of the policies that will lower the expectation include the following:

- a. Information System Security Guidelines (computer use policy),
- b. internal and e-mail use policy (including employer monitoring), and
- c. personal communication devices (company cell phones and PDAs) and voice mail policy.

Personnel policies should be adopted to provide that in order to maintain the security of its operations, the employer retains the right to access and search all work areas and personal belongings, including desks, file drawers, brief cases, handbags, pockets, and other personal effects.

In addition, the expectation of privacy is lowered when the employee is not granted exclusive control over an area. By eliminating the control, the expectation of privacy is diminished. In addition to the policy addressing the employer right to access these areas, the employer should have keys to the office, cabinets, desk, etc. The employer should require employees to provide keys to personal locks. Again, this clearly demonstrates that the employee does not have exclusive control.

These policies should also address the fact that workplace areas are subject to surveillance and that business calls may be monitored. As indicated above, the company policies should state that the employer can monitor all electronic communications, including which sites are visited over the Internet.

It is also important that the employer enforce these policies when violations are noted and enforce consistently for all known violations.

The issue of reasonable expectation of privacy is a complicated one with many variables and situations. It is strongly recommended that before an employer conducts a search or surveillance, the employer should consult legal counsel to ensure they are not violating an employee's privacy. It is also recommended that when an employer develops and implements the policies recommended here, that they have legal counsel review them in advance of implementation.

Issues regarding employer/employee rights in the workplace are certainly a complex area. By combining clear employer policies and appropriate consultation with legal counsel when issues arise, an employer can protect their ability to maintain the security of its operations.

Joseph Centofanti is a Member of the Firm and the leader of the Government Services Group at Kostin, Ruffkess & Company, LLC, a certified public accounting and business advisory firm committed to helping clients succeed. Beyond traditional accounting, auditing and tax consulting, the firm also specializes in employee benefit plan audits, litigation support, business valuation, succession planning business consulting, forensic accounting, wealth management, estate planning, fraud prevention, and information technology assurance. With 140 employees and offices in Springfield, Mass., as well as Farmington and New London, Conn., Kostin, Ruffkess serves individuals, public and private middle-market companies, not-for-profit organizations, and municipalities. Founded in 1949, the firm is celebrating its 60th anniversary this year. For more information, visit www.kostin.com or call 1.800.286.5726.