EMPLOYEE CRIME CAN COST YOU MILLIONS

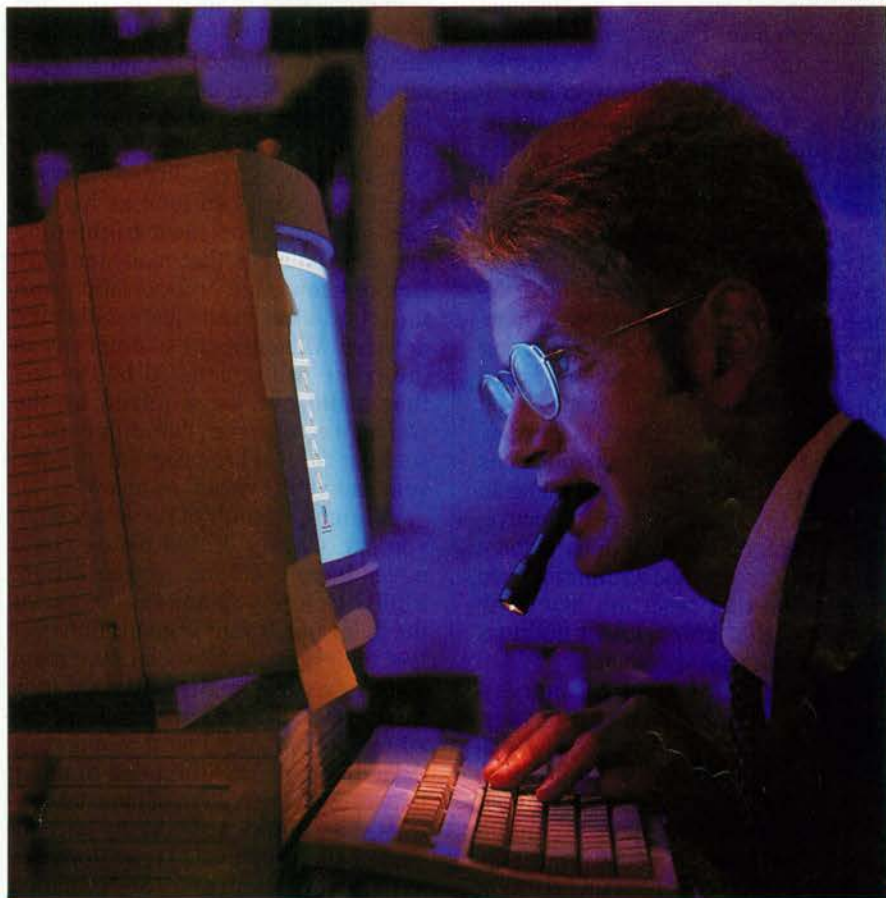
Criminal sanctions now can apply to a company—not just its employees!

BY THOMAS W. GOLDEN

Under the new *Federal Sentencing Guidelines* for organizations, your company will be held responsible if any of your employees commits a federal crime—and you can be hit with multimillion-dollar fines as punishment whether or not you or any other member of management had any knowledge of it. Although few punishments have been meted out so far, the climate is right for an upswing, and the *Guidelines* should serve as a warning that the government is serious and will act accordingly.

The *Guidelines* became law Nov. 1, 1991, out of efforts by the federal government to make responsible managements evaluate their internal control structures and make any changes that would help prevent fraudulent financial reporting and employee dishonesty. Unfortunately, many managers actually believe that fraud and other defalcations are just a "cost of doing business" and continue to defer any efforts to evaluate their existing internal control structure to identify improvements. In my view, this is exactly why the federal government has resorted to what many view as draconian effects of the *Federal Sentencing Guidelines*. Essentially what the government is saying is, "The auditors have told us they will not audit for fraud, and, therefore, Mr./Ms. Manager, the buck stops here. We don't have the money to regulate or monitor compliance under this program, but if you do not take proactive steps to clean up your own house, we will reserve the right to completely divest your organization of all of its assets should one of your employees be convicted of a federal crime."

Bob Grant



Companies must institute strong internal control systems that will prevent employee crime.

Broad in their application, the *Guidelines* cover nearly all violations of federal law and affect all organizations: corporations, partnerships, not-for-profits, governmental entities, pensions, trusts, sole proprietorships, and the like. The *Guidelines* contain *mandatory* penalties to punish—not only an employee for the commission of a federal crime, but the organization as well. No longer can an organization depend on judicial discretion in these matters.

WHAT LED TO THE GUIDELINES?

A quick review of the buildup to the *Guidelines* begins with the Foreign Corrupt Practices Act, which came on the heels of the Watergate scandal and stressed the importance for companies to develop and maintain effective systems of internal control. Then came a couple of Securities & Exchange Commission Rule proposals. One has been withdrawn because it was considered too costly, but another, introduced in 1988 and still pending action by the SEC, would require, among other things, for management to publicly acknowledge its responsibility for establishing and maintaining a system of internal control and to perform an assessment of the effectiveness of that system at least annually.

Another push toward stronger internal control came from the National Commission on Fraudulent Financial Reporting (the Treadway Commission), which, among other recommendations, said management should issue a report stating its opinion on the effectiveness of the company's internal control structure. Next was the Federal Deposit Insurance Corporation's (FDIC) Improvement Act of 1991, which, some people say, is the most demanding legislation in the area of management responsibility and reporting on internal controls to-date. Included in its provisions, which are imposed on most FDIC member banks, is for management to perform an evaluation of its internal control structure and make an assertion as to the structure's effectiveness. Management then must engage an independent public accounting firm to opine on that assertion much the same way that independent auditors opine on financial statements.

The last suggestion is Congressman Ron Wyden's (D.-Ore.) controversial Financial Fraud Detection and Disclosure Act, which passed the House (H.R. 574) but not the Senate (S. 630) in 1992. These bills, which contain identical provisions, would require independent public accountants (IPA) of public companies to use procedures in accordance with generally accepted auditing standards to detect illegal acts that have a material effect on a company's financial statements. The bills also provide for the IPA to notify the SEC of material illegal acts in circumstances where a company's management and board have failed to take the necessary remedial action and/or have failed to comply with a requirement to notify the SEC. In contrast with previous versions of the bill, the current proposed legislation maintains the responsibility for the setting of auditing standards in the private sector. Prior bills had called for the SEC to establish the "methods" to be used by the IPA to detect fraud. Accordingly, the AICPA and Big 6 accounting firms support this current proposal.

MANAGEMENT IS RESPONSIBLE

That background brings us to the *Federal Sentencing Guidelines* for organizations in which the government appears to be saying to corporate and other management something along these lines: "Come now the guidelines. We don't have the money to regulate compliance nor provide resources to monitor performance. However, what we *will* do should one of your employees or agents be convicted of a federal crime is give federal judges the power to impose fines on an organization calculated based upon a combination of the seriousness of the offense (i.e., with mandatory sentencing tables) and the culpability of the organization—which can total as high as $290 million." The most frightening part of this law is that management's lack of knowledge or association with the crime is not an adequate mitigating defense. Management's complicity in the crime will be implied by the fact that it did not, as required by the *Guidelines,* exercise due diligence in seeking to develop programs to prevent and detect violations of law.

All right, enough of the scary stuff, you say. Crimes of that nature could never happen in your organization. Right? Before you answer, consider the following. If your organization ever has undergone a financial statement audit by an independent external auditor, the auditor may have communicated to you and your board of directors or audit committee the need to maintain an effective system of internal controls. The auditor's ideas may have included such suggestions as: "Improve supervisory controls," or "enhance controls through segregation of duties" (for example, those individuals involved in the cash function should be independent of those responsible for accounts payable), or "establish codes of conduct, and implement a program to assure compliance." For what seemed at the time to be some sound business reasons—such as increased costs—you elected to defer implementation of such controls until a later period.

Combined with the recent trend in corporate downsizing, this situation has resulted in a control environment with significant weaknesses and highly susceptible to defalcations. But, basically, people are honest, right? For the most part, this statement is true. Our parents told us it wasn't right to steal. Unfortunately, persons who do confess to embezzlement, bribery, and other crimes typically rationalize the crime by convincing themselves they were not stealing. "I just borrowed the money and had every intention of paying it back...someday," or "My boss owes me this. I work harder than anyone here and therefore deserve it." These familiar themes are uttered by persons just after they confess to a wrongdoing.

WHITE-COLLAR CRIME SHOULD GET MORE PUBLICITY

If so much white-collar crime is occurring, why haven't you heard more about it? Victims of a fraud are embarrassed. Corporations and other organizations such as not-for-profit foundations aren't in a hurry to disclose to their bankers, auditors, and the public that they have been swindled. Often they elect to conduct an internal investigation, identify the culpable party or parties, and negotiate a termination settlement, which typically includes some restitution, if available, and the promise of no prosecution. The culpable parties then leave to seek other employment.

What happens when the prospective employer calls the former employer for a reference? You know the answer to that. Usually it's in the form of "Mr. Smith worked here as an assistant controller from January 1989 through March 1992." Not entirely helpful, but, with the threat of defamation, that's about all the prospective employer is going to get. Now what happens to that culpable employee in his new job? Just take a guess! And the cycle continues.

Let me add: Crimes of this nature are not committed by evil people bent on destroying their organizations. Generally they occur because of two organizational factors: *incentive* and *opportunity*. Do the following incentives sound familiar?

- Pressure to meet unrealistic performance targets, particularly for short-term results;
- High-performance-dependent rewards (bonuses);
- Group or peer pressures;

- High stress created by family or other financial needs.

Now combine those incentives with one or more of the following opportunities:

- Nonexistent or ineffective internal control system;
- Highly decentralized organization that leaves management unaware of actions taken at lower levels;
- Weak internal audit function;
- Ineffective board of directors or audit committee;
- Penalties for improper behavior that are insignificant or unpublicized and thus lose their value as deterrents.

A corporate culture that provides for incentives and opportunities such as those listed above creates an atmosphere in which a defalcation is just waiting to happen.

WHAT CONSTITUTES EFFECTIVE PREVENTION?

Fortunately, the risk of exposure to the severe penalties under the *Guidelines* can be reduced substantially if the organization has established an "effective program to prevent and detect violations of law" prior to the illegal act. According to the *Guidelines*, an effective program is a program designed, implemented, and enforced that will seek to prevent and detect violations of law. The cornerstone to the effective program is that the organization must exercise due diligence in seeking to develop such a compliance program. At a minimum, due diligence requires the organization to perform seven steps. (See "Compliance and the Tightening Legal Environment.")

Possibly the most burdensome, as well as the most beneficial, required due diligence step is providing for "reasonable steps to achieve compliance." The suggestion here is that the organization first conduct an evaluation of the existing internal control structure to assess its effectiveness—or lack thereof—then design and perform, at least annually, compliance audits to determine the extent of compliance with organizational policies, procedures, and codes of conduct. Until just recently, internal and external auditors did not have any guidance they could use as a benchmark for making an assessment of the adequacy of the internal control structure. What has changed

COMPLIANCE AND THE TIGHTENING LEGAL ENVIRONMENT

BY BRADLEY L. WILLIAMS

Michael Milken deserves some credit for the *Federal Sentencing Guidelines* for organizations and their stepchild, corporate compliance programs. Public outcry over the inside trading scandals of the late 1980s unquestionably influenced the Sentencing Commission's decision to tie future corporate criminal penalties to internal compliance efforts.

Internal regulation is not new. Corporate self-policing began with the 1934 creation of the National Association of Securities Dealers and spread to other industries on a "scandal by scandal" basis: electrical contractor bid rigging in the 1960s, foreign corrupt practices in the '70s, alleged overcharges by government contractors in the '80s, then back to the securities industry with Milken and Ivan Boesky.

Previous compliance programs were ad hoc and sporadic, existed in whatever industry was then under scrutiny, and too often were a reaction to the last problem the company faced. The sentencing guidelines change this landscape in two unprecedented ways. One, they establish a benefit for the organization that adopts them *before* a problem occurs. Two, for the first time there are overall standards defining what a compliance program should be.

The "benefit" is the mitigation of the amazingly harsh penalties which the guidelines otherwise would impose. The Exxon Valdez incident, among others, demonstrates that corporate employers are held civilly and even criminally responsible for the acts of subordinate employees. This is so even though management did not know of, much less ratify, the employee's wrongful act. Fine levels under the guidelines easily could reach millions of dollars if management were complicit in, or simply tolerated, illegal employee behavior. On the other hand, penalties are greatly reduced (to as low as 5% of the base level) for organizations that had a compliance program in place *before* the illegal conduct occurred and that report the offense and cooperate with the investigation.

Corporate compliance programs sometimes can eliminate the threat of prosecution altogether. On July 1, 1991, the U.S. Department of Justice announced that henceforth it would expressly consider voluntary compliance and disclosure efforts by companies in determining whether to prosecute environmental offenses. Self-policing carries other, less tangible, benefits ranging from improved public relations to employee morale. As one of the Milken-era defendants once put it, albeit after the fact: "Sometimes I wonder if I would still have given in to temptation if I'd had some awareness pounded into me."

To oversimplify, a compliance program consists of a code of conduct, an enforcement structure, and implementation. The code itself is the foundation of the compliance program. A typical code compiles company policy in specific substantive areas, which will vary with the organization. Popular subjects of existing codes include conflicts of interest, relations with public officials, misuse of confidential information, foreign corrupt practices, environmental compliance, insider trading, and antitrust.

Administration of the code is as important as the code itself. Effective administration requires the active involvement of the appropriate level of management. It requires communication of the code and policies to employees, training, monitoring employee conduct, establishing a reporting system for violations, consistent enforcement, and appropriate response once a violation is discovered, including internal investigations and reports of the violation to authorities.

Why the emphasis on administration? Because management may undercut the most detailed code if it conveys, even unintentionally, the impression that the rules may be ignored safely. Although employees may violate the law out of sheer ignorance, violations also may occur where the belief prevails that the conduct involved is tolerated.

The official commentary to the sentencing guidelines identifies seven factors an effective compliance program must address:

1. The organization must establish standards and procedures that are "reasonably capable" of *reducing* the prospect of criminal conduct.
2. Specific "high-level personnel"

must have overall responsibility to oversee compliance.

3. The organization must avoid delegating substantial discretionary authority to persons the organization *knew or should have known* had a propensity to engage in illegal activities.
4. The organization must communicate effectively its standards and procedures to all employees or other agents, *including independent contractors*, through training programs or publications.
5. The organization must take reasonable steps to achieve compliance with its standards, for example, by utilizing monitoring and auditing systems reasonably designed to detect employee criminal conduct and by publicizing a reporting system whereby employees and agents may report criminal conduct by others.
6. Standards must be enforced consistently, including discipline of employees who fail to report an offense. "Adequate discipline of individuals responsible for an offense is a necessary component of enforcement."
7. After an offense has been detected, the organization must take all reasonable steps to respond appropriately to the offense and to prevent further offenses, including necessary modifications to the compliance program.

Other commentary suggests that the compliance program should take into account the size of the organization, the likelihood that certain types of offenses may occur because of the nature of the business, and the history of the organization. The failure to incorporate and follow standard industry practice, or any standard called for by a government regulation, "weighs against a finding" that the program was effective.

Employees should be encouraged to report claimed violations of the code or the law to their immediate supervisor. There should also be a procedure for confidential reporting outside the normal chain of command. Companies with compliance programs often designate corporate counsel, internal audit personnel, or a separate company ombudsman to receive these reports.

All this may be a lot for bottom-line-conscious boards of directors to absorb, especially for something that may be viewed simply as protection against the worst case. In a broader sense, a compliance program institutionalizes the organization's response to adverse situations while they still are controllable. A compliance program cannot prevent every violation. It *can* do a lot to ensure the violation will be seen for what it is: the aberrant act of an employee and not an outgrowth of company policy. In the current law enforcement climate, that may make an enormous dollars-and-cents difference to the corporation and its shareholders. ■

Bradley L. Williams is of counsel to the Indianapolis law firm of Ice Miller Donadio & Ryan, where he has practiced since 1988. He served as a federal prosecutor for 10 years, including service as first assistant United States Attorney and as acting United States Attorney for the Southern District of Indiana.

the manner in which such an evaluation can be performed is a new report titled *Internal Control—Integrated Framework*, which was developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. Already called a landmark, the study establishes a standard for internal control effectiveness for use by all parties involved with internal controls. The three-year study involved thousands of hours of research, discussion, analysis, formal dialogue, and due process. Many hundreds of people—including many members of the sponsoring organizations, chief executives, board members, legislators, regulators, lawyers, consultants, and academics—participated.

An outgrowth of a Treadway Commission recommendation, the project is a further initiative of the five organizations that sponsored Treadway (the Institute of Management Accountants, the American Institute of CPAs, the Financial Executives Institute, the Institute of Internal Auditors, the American Accounting Association). It was initiated to deal with the lack of a common, accepted definition of what internal control is or does. Miscommunication and different expectations of internal control have been rampant.

COSO undertook this project to define and integrate internal control concepts and to provide a common language and reference point. The objective was not only a conceptual framework but also a standard against which companies could assess their internal control systems and judge their effectiveness. In other words, the study was to provide a common language and understanding as well as a practical way for companies to assess and improve their control systems. It has succeeded, and it provides an outstanding section of practice aids that will enable management as well as external auditors to perform this evaluation.

Now company managements should perform such an evaluation of their internal control structure in accordance with the framework of the COSO study. In an effort to save costs, many managements undoubtedly will attempt to perform this evaluation themselves without retaining the services of outside consultants. This is an age-old issue and should be considered carefully. I contend that in most cases management is too close to the situation and cannot possibly and realistically perform an objective evaluation of their own systems. If you really want to find the dirt in your house, invite your next-door neighbor to walk through it and point out all the cobwebs and dust. My suggestion: Don't do it yourself; you'll miss the obvious.

COMPLY...OR ELSE

Although the *Guidelines* became law in late 1991, there have not been any significant sentences to-date because the investigation and prosecution process takes an extensive period of time. I have been told by members of the legal profession that we should expect to see some significant prosecutions under the *Guidelines* in late 1993 and many more in 1994. When businesses see their competitors splattered all over the front page of the morning paper, they will become more proactive in response to the due diligence steps required under the *Federal Sentencing Guidelines*. They can only hope that it is not their business that ends up on that front page first.

Executives cannot sit back and ignore the *Guidelines*. There are many in other professions that would disagree with this comment, but I believe that the COSO framework will do for internal control structures what accounting pronouncements have done for financial statements. When a reader picks up a set of financial statements, that reader gains a tremendous amount of confidence in the information contained therein when the words "generally accepted accounting principles"

are included. The COSO study framework has taken a tremendous leap in attempting to render to financial statement readers that same level of comfort. I believe the issue will be put to bed once interested parties (investors, banks, the public) have an opportunity to view the result of how a new attestation standard issued by the AICPA is utilized by managements and external auditors engaged to opine on management's assertion of the effectiveness of an entity's internal control system. The new Statement, *Reporting on an Entity's Internal Control Structure Over Financial Reporting*, is effective for an examination of management's assertion on the effectiveness of an entity's internal control structure over financial reporting when the assertion is as of December 15, 1993, or thereafter. As always, earlier application of the Statement is encouraged.

Unfortunately, very few of the executives with whom I talk are aware of the *Federal Sentencing Guidelines*, the COSO study, or other information. My only hope is that the word gets out before the indictments do. ■

Thomas W. Golden, CFE, CPA, is the director of litigation & claims services for Coopers & Lybrand's Indiana/Ohio/Kentucky Cluster and resident in Indianapolis. He is directly responsible for providing expertise to attorneys, law firms, insurance companies, law enforcement agencies, prosecutors, and corporations. He may be reached at (317) 639-4161.

Is this article of interest to you? If so, circle appropriate number on Reader Service Card. Yes 66 No 67

WANTED: CORPORATE COPS

After several particularly complicated investigations, noted criminologist Dr. Donald R. Cressey remarked, "America needs a new kind of corporate cop." Dr. Cressey was a student of the man who coined the term "white-collar crime" and conducted much original research on the subject. Now, years after his death in 1987, the force he had envisioned is a reality—the Certified Fraud Examiner (CFE).

These specialists in the detection and/or deterrence of fraudulent activity are employed by most major corporations and governmental agencies to investigate allegations of misconduct from discovering employees or executives who misappropriate company assets to assisting investors who have been defrauded in commercial transactions. The private sector uses CFEs for investigative and consulting services in the areas of litigation support and fraud investigation and prevention. Their duties are numerous: obtaining evidence, taking statements and writing reports, testifying, giving advice on how a company can prevent fraud in the future, and more. CFEs can help organizations police themselves.

According to the Association of Certified Fraud Examiners, which was founded in 1988 by Joseph T. Wells, its current chairman, CFEs must meet certain educational and experience requirements, must exemplify the highest moral and ethical standards, must agree to adhere to the group's code of professional ethics, and must pass the rigorous Uniform CFE Examination that tests knowledge in the areas of financial transactions, investigation of fraud, criminology and ethics, and legal elements of fraud. (The group's address is ACFE, 716 West Avenue, Austin, TX 78701, 1-800-245-3321, phone, (512) 478-9297, fax.)

Here are some examples of their activities:

- A CFE in private practice was retained to examine evidence of fraud and to testify in a $350-million securities fraud case. His testimony helped his clients recover $70 million.
- A CFE in the internal audit department of a bank headed the investigation of a $125,000 embezzlement case. She ultimately assisted in the criminal prosecution of an officer.
- A CFE employed by the government advised a federal agency on ways to improve its ability to detect fraud in contracts, which resulted in potential savings of millions of dollars.

Author Tom Golden is one of the new corporate cops. He became a CFE as a natural outgrowth of his auditing work at Coopers & Lybrand. He had joined the firm "rather late in life," he says, at age 31 "with experiences that enabled me to be well-suited to be assigned as a staff person on some of the firm's more risky clients. With only one year of experience with the firm, I uncovered a financial statement fraud which appeared to be tied to the top executives of this public company. Upon identifying indications of possible defalcations, I led a 17-week investigation that was later used by the Securities & Exchange Commission in its investigation of this company's activities. This experience essentially set me upon a career path, ultimately drawing me more and more into the area of fraud and forensic investigations."

Each time a similar situation arose, Tom was assigned to the matter. Two years ago, when he was promoted to director of litigation & claims services for C&L, a colleague suggested he become a CFE. He applied to the ACFE and was accepted under the group's "advance standing" program whereby individuals who met the training, education, and experience requirements could become CFEs without taking the exam. (The program expired Dec. 31, 1992.)

As a CFE and CPA, Tom works fulltime with trial lawyers, corporate counsels, and managements on technical, business, industry, acounting, and financial issues; damage claim analysis and review; economic analysis and special market studies; forensic investigatory accounting; and fraud investigations. He has testified as an expert witness in both civil and criminal matters and has developed special expertise in forensic investigatory accounting, fraud investigations, and internal control evaluations.

Here are some of the projects on which he has worked:

- A public company engaged him to conduct a forensic investigation to determine if certain members of executive management were fraudulently falsifying documents and records to create new leasing customers. His investigation resulted in the company's treasurer pleading nolo contendere to charges by the SEC of financial statement fraud (Treadway Commission fraud). Tom was the lead witness for the SEC, giving aproximately 25 hours of deposition testimony before rep-

resentatives of the SEC over the two-year investigation period. This case was similar in scheme to the Equity Funding Insurance Company of America fraud perpetrated in the late 1970s and popularized in the videotape, *The Billion Dollar Bubble*.

- A real estate developer engaged Tom to conduct a covert fraud investigation of his partner in a Florida condominium project. After just several days of investigation, it was determined that his partner had embezzled substantial amounts of cash through various schemes. At the request of the client, Tom presented his findings in a formal written report whereupon the culpable party made restitutuion and no criminal charges were pursued.
- Tom conducted a fraud investigation of a high-tech electronics manufacturer whereby the controller was dismissed after some questionable transactions came to the CEO's attention. After completing the investigation and documenting the results in an evidence package, Tom presented it to detectives with the local police, who in turn interviewed the controller. Not being able to extract a confession, the police and the county prosecutor asked Tom to interview the controller. During that interview, the controller confessed to seven counts of felony theft and forgery.
- A diversified insurance company engaged Tom to review the accounting records of a property management company where the insurance company had a participating mortgage on the property. There were no irregularities noted, but this investigation helped clarify some contract interpretation issues such that the parties had a clearer understanding about the method in which cash flows would be distributed.

Author Tom Golden.

One of Tom's latest cases involving the federal sentencing guidelines is having a different conclusion from most of his investigations. An internationally recognized not-for-profit group engaged him to investigate certain financial transactions conducted by a director of the organization. During the investigation, he identified a pattern of deception and deceit that appeared to involve the director acting without board authority to solicit contributions from benefactors in a number of states, the funds of which were deposited into a secret bank account. "The Board had directed me to conduct an investigation whereupon I developed the evidence package, did an interview/interrogaton of the director, and obtained a confession regarding the misappropriation of Foundation funds." After negotiations with the Foundation's attorneys, the director terminated her association with the Foundation and provided significant restitution, while the Foundation's Board agreed not to prosecute with state or federal authorities. Both parties walked away feeling they had accomplished their objectives.

"Shortly thereafter," Tom explains, "One of the Foundation directors, either by intention or inadvertently, discussed the matter with a special agent of the FBI. When the FBI learned from this director that I had conducted the investigation, they walked into my office accompanied by a criminal investigations officer with the IRS and handed me a subpoena to appear before a federal grand jury.

"The Board requested me to attend a meeting to discuss what implications this could have. Their concern was one of doubt as to the U.S. attorney's office intentions—was the office considering criminal action against the Board under the federal sentencing guidelines? I couldn't answer. Fortunately for the Board, later discussions with the FBI and the atorney's office indicated the U.S. attorney believed the Board was a victim in this matter and was not intending to pursue criminal indictment of the Foundation.

"At the conclusion of my grand jury testimony, the U.S. attorney asked the jurors if they had any questions for me. One particularly insightful one should serve as a warning to all organizations: A kindly old lady raised her hand. 'I want to know where the Board was during the embezzlement. Where were the checks and balances that we should come to expect from such a group of individuals? Were they not doing their job?'

"I answered, 'That is a good question, but consider that this was a new foundation composed entirely of noncompensated directors. They were helping start what they felt was a charitable organization with commendable goals and objectives, but doing so in their spare time much the same way you and I might serve on a committee for our church or social organization. I believe the Board acted responsibly when they learned there may be improprieties and engaged me to conduct an investigation to determine if there was a basis for those concerns.' The U.S. attorney agreed the Board was a victim and with those comments most likely stopped what could have been a runaway grand jury who may have decided on their own to pursue an investigation against the Board under the federal sentencing guidelines.

"I believe the government intends to package up my testimony with a budget for the continuance of this investigation to the Justice Department in Washington, D.C., for approval. I expect they will subpoena other witnesses, with the possibility for any indictments being handed down not until October or November of this year."

Companies now have been warned and should start strengthening their internal control systems immediately if they have been waiting for some sign of government direction. The indications are clear. ■