Bloomberg BNA

Daily Report for Executives™



Corporations

Authors Kristin Graham Koehler and Brian P. Morrissey say that creating a compliance program that conforms to the Sentencing Guidelines mandate can be a complicated task for companies in the retail industry who are required to comply with dozens of federal regulatory regimes enforced by numerous federal agencies.

But the benefits are impressive, including cutting the likelihood that the company will ever face criminal liability and significantly reducing any penalties if a case is brought.

# Developing Solid Compliance Programs for Retailers: Challenges and Benefits

KRISTIN GRAHAM KOEHLER AND BRIAN P. MORRISSEY

## I. Introduction

Developing an effective compliance program presents retailers in today's regulatory and enforcement environment with a substantial challenge—and a critically important opportunity. The U.S. Sentencing Commission's Organizational Sentencing Guidelines (the ''Guidelines'') establish the bar for determining the sufficiency of an organization's compliance program. Creating a program that conforms to the Guidelines' mandate can be a complicated task, especially for companies in the retail industry. Due to the breadth and diversity of their business operations, retailers are often required to comply with dozens of federal regulatory regimes and are often subject to enforcement by numerous federal agencies. Each of those agencies has a somewhat different view of the ideal compliance program, and crafting a program that meets all of their standards, as well as the Guidelines, can be a challenging endeavor.

Yet if this hurdle is overcome, an effective compliance program can offer a retailer invaluable rewards. Most importantly, an effective program will reduce compliance gaps and decrease the likelihood that the company will ever face criminal liability. In addition, if a legal violation occurs, having an effective compliance program in place can significantly reduce the penalties a company would otherwise face. Indeed, if a company is convicted of a crime, but had an effective compliance program in place at the time of the misconduct, the U.S. Sentencing Commission reports that the potential fine range can be reduced by up to 95 percent.[1] Moreover, if a company is investigated for potential misconduct, evidence that it had an effective program may stave off a criminal prosecution completely. As a matter of policy, federal prosecutors and regulators consider compliance programs when making enforcement decisions, and a

**Kristin Graham Koehler** *is a partner in the Washington, D.C., office of Sidley Austin LLP, where her practice focuses on the representation of corporations and individuals in all phases of government enforcement matters, including internal investigations, grand jury proceedings, and trials. She has significant experience in developing corporate compliance and audit programs in a broad range of industries.*

**Brian P. Morrissey** *is an associate in the Washington, D.C., office of Sidley Austin LLP, where his practice focuses on white collar and complex civil litigation matters and appeals.*

[1] Ethics Resource Ctr., *The Federal Sentencing Guidelines For Organizations At Twenty Years* 22 (2012) (''ERC Report''), *available at* http://www.ethics.org/resource/federal-sentencing-guidelines-organizations-twenty-years (citing U.S. Sentencing Commission, FY 1992- FY 2010).

strong compliance program can provide a company with an essential tool when defending itself against charges of wrongdoing.

This article examines the key elements of an effective compliance program for a company in the retail industry, the challenges associated with developing such a program, and the important benefits of doing so.

## II. The Elements of an Effective Compliance & Ethics Program

### A. General Principles

The Guidelines set forth in detail the elements of an effective compliance program, thus providing an essential template for any company seeking to build one.[2] The Guidelines were promulgated and became effective in 1991 as part of an effort to eliminate perceived disparities in sentencing for federal crimes and a perception that courts were sentencing certain types of defendants too lightly.[3] The Guidelines establish a set of principles for federal courts to use in setting criminal sentences.[4]

**A company is liable for the wrongful acts of its employee so long as the employee is acting in an official capacity, even if the employee acted contrary to corporate policy and instructions.**

The Guidelines embrace the principle that an organization is liable for the wrongful acts of its employee so long as the employee is acting in an official capacity, even if the employee acted contrary to corporate policy and instructions. As a consequence, ''[a]n entire organization, despite its best efforts to prevent wrongdoing in its ranks, can still be held criminally liable for any of its employees' illegal actions.''[5] Furthermore, the Guidelines aim to deter corporate misconduct by setting penalties for organizational defendants at higher levels than judges typically had imposed before 1991.[6]

Importantly, however, in addition to the increased penalties, the Guidelines offer organizational defendants important incentives. Most relevant here, the Guidelines authorize a significant reduction in penalty for an organization that demonstrates it had an effective ''compliance and ethics program'' in place to prevent and deter legal violations at the time the misconduct occurred.[7] Under the Guidelines, the fine imposed on an organizational defendant is calculated by multiplying a base fine by two multipliers determined by a ''culpability score.''[8] The ''culpability score'' is calculated by adding points for aggravating factors, such as obstruction of justice or recidivism, and by subtracting points for mitigating factors, such as acceptance of responsibility and the existence of an effective compliance program.[9] The existence of an effective compliance program, therefore, has a direct and potentially substantial effect on the fines to which a corporate defendant is exposed.

As adopted in 1991, the Guidelines provided guidance on what constitutes an effective compliance program. The Guidelines have been amended twice in the last eight years—in 2004 and again in 2010—to provide further clarity regarding the contours of an effective compliance program. The 2004 amendments clarified that an organization's compliance and ethics program must have seven specific elements, described below. The 2010 amendments further refined those elements. As a general overarching mandate, the Guidelines require that companies ''exercise due diligence to prevent and detect criminal conduct'' and ''otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.''[10] In short, a compliance program should be a comprehensive management system designed to create and promote a culture of ethical conduct and to prevent, detect and correct violations of law.

### B. The Seven Necessary Elements of an Effective Compliance Program

It is virtually impossible to prescribe a ''one-size-fits-all'' compliance program for companies in any industry, especially retail. Most retailers have broad and diverse business lines, and face a multitude of federal regulatory requirements at each phase of their operations, including merchandising, advertising, supply chain management, and human resources, to name just a few. The first step in developing an effective compliance program is to identify the substantive laws with which the retailer must comply. Examining federal law alone, most retailers have obligations to comply with securities, environmental, labor, worker safety, anti-bribery, and anti-money laundering regulations, a list that just scratches the surface. State regulations and (for multinational retailers) foreign legal requirements must also be considered. This article does not endeavor to describe the specific steps necessary to comply with each of these substantive legal regimes. The substantive bod-

[2] In 1984, Congress passed the Sentencing Reform Act, Pub. L. No. 98-473, 98 Stat. 1987, which created the Sentencing Commission. The Commission submitted its proposed Sentencing Guidelines for individuals to Congress in 1987 and submitted its proposed Sentencing Guidelines for organizations to Congress in 1991. *See* U.S. Sentencing Comm'n, Guidelines Manual (''Guidelines Manual''), Chapter 8, Sentencing of Organizations (Nov. 1, 1991).

[3] Organizations covered by the Guidelines include any corporation, partnership, association, joint-stock company, union, trust, pension fund, unincorporated organization, government or political subdivision of a government or nonprofit organization. Federal Sentencing Guidelines, codified at 18 U.S.C.A. § 8A1.1. (Cmt. West 2007).

[4] In 2005, the Supreme Court held that requiring courts to impose sentences based on the Guidelines violated the Constitution. *United States v. Booker*, 543 U.S. 220 (2002). Nevertheless, the Supreme Court held that sentencing judges should use the Guidelines in an advisory fashion, signaling their continuing viability and relevance.

[5] Paula Desio, Deputy Gen. Counsel, U.S. Sentencing Comm'n., *Introduction to Organizational Sentencing and the U.S. Sentencing Commission*, 39 Wake Forest L. Rev. 559, 560 (2004).

[6] *Id.*

[7] Guidelines Manual § 8C2.5(f) (2009).

[8] *Id.* §§ 8C2.4(a), 8C2.7.

[9] *Id.* § 8C2.5.

[10] U.S. Federal Sentencing Guidelines (''Guidelines''), codified at 18 U.S.C.A. § 8B2.1.(a).

   ISSN 0148-8155

ies of law by which a particular retailer must abide will be determined by the particular scope of its business.

Yet regardless of the lines of business in which a particular retailer is engaged, and regardless of the substantive bodies of law with which it must comply, the *structure* of an effective compliance program is largely constant. An effective compliance program for any retailer—or any U.S. organization for that matter—must contain the following seven elements, as prescribed by the Guidelines.

### 1. Standards and Procedures

The Guidelines require that the organization ''establish standards and procedures to prevent and detect criminal conduct.''[11] This typically means that the organization must have a written Code of Conduct and/or Code of Business Ethics reflective of the organization's expectations for employee behavior.[12] In addition, the company must have standards and procedures reasonably capable of reducing the prospect of criminal conduct. At bottom, this is a common sense requirement: if the Board and senior management expect people to do the right thing, it is important to communicate, through standards and procedures, what the right thing is and how it can be accomplished. Once expectations are made clear, management can then fairly enforce the program.

Procedures should provide practical direction designed to make sure that people know precisely what (and what not) to do. Procedures should be evaluated from the perspective of the ultimate user, not the ''experts'' who write the procedures. Detailed procedures that may be legally or technically correct are often not effective because they either do not fit the practical day-to-day context of the employees or the employees simply cannot understand them. For example, lengthy memoranda on antitrust law simply will not be read by a busy, hard-charging sales force in the field, who is frequently interacting with competitors. Concise, practical guidance, however, will be and, therefore, is imperative.

One approach is to build compliance objectives into regular business practices, such as including questions about money-laundering on transactional documents or about employee rights on human resources documents. Where business processes are computerized, mandatory electronic compliance ''check-offs'' also can be added. This approach can reinforce compliance in an everyday way, rather than relying solely on policy documents.

### 2. Leadership and Oversight

The Guidelines establish three senior levels of responsibility for compliance programs: (a) governing authority; (b) high-level personnel; and (c) ''specific individuals.''[13]

#### a. *Governing Authority*

The ''governing authority'' is the highest-level governing body of an organization, typically its Board of Directors. The Guidelines provide that the organization's governing authority ''shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the . . . program.''[14] In short, the Guidelines impose an explicit responsibility on the Board of Directors to know how the compliance program works and to oversee its implementation. This is designed to require a ''culture of compliance'' at the highest levels of the organization.[15]

While the Guidelines do not specify how the Board should meet these obligations, the oversight function is often assigned to a committee of the Board such as the Audit Committee or the Ethics and Compliance Committee. Regardless of how Board oversight is organized, the Board should review and approve the key elements of the compliance program and exercise regular and visible oversight.

#### b. *High-Level Personnel*

The Guidelines further require that ''[h]igh-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program.''[16] Thus, all management, not just those formally charged with compliance, must be knowledgeable about the operation of the compliance program and perform their duties in a manner designed to prevent and detect violations of the law and promote an organizational culture that is committed to compliant and ethical conduct. This means that each manager needs to understand the legal issues and the company's policies relevant to the work of the relevant business unit and

[11] *Id.* § 8B2.1(b)(1).

[12] Multinationals that are publicly traded in the U.S. and operate in the European Union must consider data protection, labor, and human rights laws in the relevant jurisdiction in implementing an employee Code of Conduct. For example, efforts to implement a binding Code of Ethics or employee Conduct Code could result in breach of EU labor law, or the domestic labor laws of certain EU countries.

[13] Guidelines § 8B2.1(b)(2).

[14] *Id.* § 8B2.1(b)(2)(A).

[15] This Guidelines requirement is consistent with Delaware Supreme Court precedent, which has broadly suggested that individual members of Boards of Directors have a fiduciary duty to ensure that an organization acts in compliance with applicable laws and has a compliance program to meet this obligation. *In re Caremark Int'l Inc. Deriv. Litig.*, 698 A.2d 959, 970 (Del. Ch. 1996) (''[A] director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards.''). The Delaware Supreme Court has further held that directors may be liable for failure to exercise oversight if the directors failed utterly to implement any reporting system or controls or, having implemented such a system, consciously failed to monitor or oversee its operations, and thus, prevented themselves from being informed of the risks or problems requiring their attention. *Stone v. Ritter*, 911 A.2d 362 (Del. 2006); *In Re Walt Disney Co. Deriv. Litig.*, 906 A.2d 27 (Del. 2006).

[16] Guidelines § 8B2.1(b)(2)(B).

ensure that employees under their management or supervision understand and follow those procedures.

**Some organizations make the general counsel the compliance officer, although . . . this can impose an overly legalistic tone to the program and might discourage internal communication about ethical issues, given some employees' reluctance to talk to lawyers.**

According to the Guidelines, ''[s]pecific individual(s) within high-level personnel shall be assigned overall responsibility for the . . . program.''[17] While the Guidelines do not use the term ''compliance officer'' or ''ethics officer,'' the person who is assigned this responsibility often carries such a title. Ethics or compliance officers can report directly to the CEO or the Board (or both). Alternatively, ethics or compliance officers are sometimes incorporated into the legal function and report to the general counsel, although the government discourages that approach.

There are many approaches to organizing the compliance function. One is to appoint a senior operating manager as the compliance and ethics officer, sending the clear message that ethics and compliance are core business values. Another is to put an ''ethics professional'' in that role. This potentially emphasizes ''independence,'' although it may unintentionally create the impression that ethics is a staff responsibility separate from normal business operations. Some organizations make the general counsel the compliance officer, although concerns have been raised that this can impose an overly legalistic tone to the program and might discourage internal communication about ethical issues, given the reluctance of some employees to talk to lawyers. Another option is to have a ''compliance committee'' composed of executive management that oversees the operation and performance of the compliance system. Regardless of how the compliance function is organized, someone must be assigned overall responsibility for the program.

**The Guidelines provide special protocols for cases in which high-level personnel is involved in criminal misconduct.**

The Guidelines also provide protocols for cases in which high-level personnel is involved in criminal misconduct. Prior to 2010, the Guidelines did not permit a deduction from the organization's culpability score—regardless of the effectiveness of its compliance program—if high-level personnel participated in, condoned, or were willfully ignorant of the offense.[18] Under the 2010 amendments, such misconduct by high-level personnel no longer automatically prevents a deduction in the organization's culpability score. Instead, an organization retains a pathway to a deduction, even if high-level personnel were involved in the misconduct, if the organization has an effective compliance program and can establish the following four facts : (1) the personnel involved in the misconduct did not have operational responsibility for the compliance program; (2) the individuals with operational responsibility for the compliance program have ''direct reporting obligations'' to the highest governing authority of the organization or an appropriate delegate thereof;[19] (3) the compliance program detected the misconduct before it was discovered outside the organization or before such discovery was reasonably likely; and (4) the organization promptly reported the misconduct to appropriate governmental authorities.[20]

**c. *Specific Individuals***

The Guidelines mandate that

> [s]pecific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.[21]

Accordingly, day-to-day responsibilities for the compliance program may be delegated to levels below the senior manager who is serving as the compliance officer. For example, drafting procedures, conducting training and audits, operating an ethics hotline, or collecting and summarizing performance information may be done by staff reporting to the compliance officer. The senior compliance function also may be supported by a cross-functional compliance staff team (e.g., human resources, legal, finance, or audit) that assists on the day-to-day operation of the compliance program. Some of the work might also be delegated outside the compliance function. For example, some companies delegate the investigation of non-critical hotline calls to their human resources department.

[17] *Id.* § 8B2.1(b)(2)(B).

[18] *Id.* § 8B2.1.

[19] Pursuant to the comment note to this Guidelines provision, an individual has ''direct reporting obligations to the highest governing authority of the organization if the individual has ''express authority to communicate personally to the governing authority or appropriate subgroup thereof (A) promptly on any matter involving criminal conduct or potential criminal conduct, and (B) no less than annually on the implementation and effectiveness of the compliance and ethics program.'' *Id.* § 8C2.5, cmt. 11

[20] *Id.* § 8C2.5(f)(3)(C).

[21] *Id.* § 8B2.1(b)(2)(C).

   ISSN 0148-8155

**The importance of making resources available to support compliance cannot be overestimated.**

Persons to whom such day-to-day compliance responsibilities have been delegated must be provided adequate resources and authority to do their jobs, and must also report periodically to senior management on the effectiveness of the program. The Commission emphasized that while various duties may be delegated, ultimate responsibility for the effectiveness of the compliance program resides in senior management. The importance of making resources available to support compliance cannot be overestimated. If people do not have time to do their jobs, and performance goals continue to climb, the temptation to cut corners on ''soft'' issues such as compliance and ethics increases. If compliance and ethics are treated as something people must pay attention to in their spare time, the company will have a ''spare time'' quality program.

The Commission commented that if the compliance officer does not have day-to-day responsibilities for the program, then the person(s) with the day-to-day responsibilities should report directly to the Board, or a Board Committee, at least annually on the effectiveness of the program. The goal here is that senior management and the Board (or a committee thereof) should periodically hear from people ''in the trenches'' about how the compliance program is actually working.

In summary, the Board as well as senior and mid-level management are responsible for the compliance program's implementation and oversight, must understand how the program works, provide it with adequate funding and resources to be effective, and cannot simply shift these responsibilities to staff. Day-to-day compliance operations, however, may be handled by lower-level employees, provided that they have direct access to senior management.

### 3. Individuals with Substantial Authority in the Organization Cannot Have a Propensity to Act Criminally or Unethically

Under the Guidelines, the organization must ''use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.''[22] ''Substantial authority personnel'' include senior managers, as well as individuals who exercise substantial supervisory authority (*e.g.*, a plant manager or a sales manager).

There is no absolute bar on hiring individuals with a history of misconduct in positions of responsibility. Further, the commentary adds that the Guidelines are not intended to authorize behavior that would be inconsistent with state hiring laws, including laws that prohibit discrimination based solely on a person's arrest record. The organization, however, should take into account whether the individual's record of misconduct relates (or does not relate) to the individual's anticipated responsibilities, as well how recent the misconduct was in determining whether to hire the individual.

### 4. Communication and Effective Training

As previously discussed, the Guidelines place strong emphasis on the need for organizations to have a documented compliance program, but having a program on paper alone (i.e., ''a paper tiger'') is insufficient. Indeed, this has been a consistent point of emphasis for prosecutors and regulators. The Chief of the Department of Justice's (''DOJ'') Criminal Division has warned against instituting ''paper'' programs that fail to develop adequately a ''true culture of corporate compliance,''[23] and a former Director of the Securities and Exchange Commission's Division of Enforcement has urged corporations not to ''fall victim to a checklist mentality.''[24] Instead, the program must be communicated to and utilized by employees within the organization. Simply distributing a copy of the Code of Conduct to employees is only the first step; effective training must follow.

The Guidelines provide that ''[t]he organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program . . . by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.''[25] Specifically, these communications should be made to: members of the governing authority (Board of Directors); high-level personnel; substantial authority personnel; the organization's employees; and, as appropriate, the organization's agents.

The objective of effective training programs is straightforward: the participants need to understand the company's expectations regarding ethical and compliant conduct, their roles and responsibilities regarding such conduct, and when and where to seek assistance. It is particularly important that the training be relevant and specifically targeted to the participants' work responsibilities; generalized training is rarely effective.

[22] *Id.* § 8B2.1(b)(3).

[23] Lanny A. Breuer, Assistant Attorney General, Criminal Division, U.S. Department of Justice Prepared Remarks to Compliance Week 2010 – 5th Annual Conference for Corporate Financial, Legal, Risk, Audit & Compliance Officers May 26, 2010, www.justice.gov/. . ./pr/. . ./05-26-10aag-compliance-week-speech.pdf.

[24] Stephen M. Cutler, Dir., Div. of Enforcement, U.S. Sec. & Exch. Comm'n, Second Annual General Counsel Roundtable: Tone at the Top: Getting it Right (Dec. 3, 2004), *available at* http:// www.sec.gov/news/speech/spch120304smc.htm (quoting Richard C. Breeden, Restoring Trust: Report to The Hon. Jed S. Rakoff, the United States District Court for the Southern District of New York, on Corporate Governance for the Future of MCI, Inc. 30 (Aug. 2003), *available at* http:// news.findlaw.com/hdocs/docs/worldcom/ corpgov82603rpt.pdf).

[25] Guidelines § 8B2.1(b)(4).

**Effective training requires employees to think through complex "gray areas" that employees may encounter in the workplace.**

In addition, effective training requires employees to think through complex ''gray areas'' that employees may encounter in the workplace, instead of merely advocating the significance of ethical behavior. Effective training provides employees a clear set of practical tools for identifying, navigating, and resolving ethical dilemmas, particularly, in situations where it is difficult to balance competing interests or determine the right thing to do. Such training should be interactive and provide realistic examples of the ethical dilemmas that employees may encounter as they perform their job duties.

Also critical to gaining employee support of any code of ethics is training that communicates the organization's commitment to an ethical culture. For example, if a high-ranking official in the organization introduces the online or video-based training, and explains the critical importance of compliance to the organization, this will demonstrate management's commitment to compliance. Additionally, in order to encourage employees to report ethical misconduct, they must understand that the organization will follow-up on reports.

The Guidelines commentary states that small organizations (those with fewer than 200 employees) may provide training through informal mechanisms, such as informal staff meetings, as long as the informal trainings effectively communicate the organization's compliance and ethics standards and procedures. But, larger organizations must provide more formal programs. In addition, organizations must do more than provide a one-time training to their new employees. The Guidelines comment that the communication and training requirement is ongoing, requiring ''periodic'' updates, most likely, in conjunction with the organization's duty to periodically evaluate the program's effectiveness. Obviously, forcing employees to take the same training course repeatedly is less effective than instead refreshing employees on the topics of major importance previously covered and introducing new developments in relevant law and organizational policies.

Compliance and ethics training should address situations where employees may, perhaps without knowing, violate a law or organizational policy and thereby expose the organization to liability and reduced morale and productivity. In addition, an organization may likely need to provide its employees with compliance and ethics training relating to its particular industry and the nature of its workforce. For example, training for many employees in the retail industry may need to cover some, if not all, of the following topics in their training program: confidential information, proper accounting, organizational property, gifts and favors, fair labor standards, unfair trade practices, Americans With Disabilities Act (''ADA'') rules, sexual harassment, outside employment, and reporting. Also, directors and high-ranking personnel will need additional guidance on their specific duties under relevant laws and regulations. Training should focus not only on the law, but also explicitly explain the organization's policies on specific subjects.

**5. Monitoring, Auditing, and Disclosure**

Under the Guidelines, ''[t]he organization shall take reasonable steps (A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct; (B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and (C) to have and publicize a system . . . whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation'' through ''anonym[ous] or confidential[]'' means.[26] In other words, the company must take reasonable steps to ensure that the compliance program is being implemented and followed, and that effective channels exist through which employees and agents may report misconduct.

The building blocks to implementing a strong compliance program are (1) developing monitoring and auditing procedures to detect illegal conduct, and (2) instituting periodic evaluations of the effectiveness of the compliance program. Setting measurable goals, with defined objectives to work toward is a key step in this process. Furthermore, the strength of a company's auditing program is crucial to demonstrating to government regulators or enforcers that it has a credible compliance program, as opposed to a ''paper'' program. If a company is not looking hard at its own conduct, the government will assume that it does not take the program seriously and is not interested in detecting problems. It is always better for a company to find a problem before someone else does (particularly, the government), or before a whistleblower or former employee publicly broadcasts it. Auditing also demonstrates to employees and agents subject to the compliance program that the company takes seriously the commitment to compliant and ethical conduct.

Once a strong compliance program is in place, effectively auditing the program is critical to maintaining its success. Auditing a compliance program typically involves (1) verifying that the elements of the program are in place and (2) obtaining objective evidence through interviews, document reviews, and observations that the program is actually being implemented.[27] For example, program audits would not only try to determine whether unfair trade practices have occurred, but rather assess the existence and effectiveness of procedures designed to prevent such practices, management leadership on such issues, etc. These audits can often catch potential issues before they turn into real problems because they focus on the extent to which employees and agents understand what they are supposed to do and whether they are doing it, and not just on the narrower issue of compliance. In the event questionable activities have occurred, the review would include a systems review to determine why the potential misconduct occurred and why was it not detected and reported (*i.e.*, root cause analysis).

---

[26] *Id.* § 8B2.1(b)(5).

[27] The internal audit team and chief compliance and ethics officers should study the various guidance that is available. One might start by reviewing the ''Open Compliance and Ethics Group (''OCEG'') Internal Audit Guide'' for auditing a compliance and ethics program, which is available at www.oceg.org.

   ISSN 0148-8155

**Program reviews increasingly include assessments of "corporate culture" . . . what managers, employees, contractors and others think, . . . what motivates them, what are the "unwritten rules" on how "things really work."**

Program reviews increasingly include assessments of "corporate culture." These reviews explore what managers, employees, contractors and others think about the organization, what motivates them, what are the "unwritten rules" on how "things really work," what they believe is acceptable and unacceptable behavior, whether they feel comfortable raising concerns or questions or feel pressures to get the job done and cut corners, etc. Such reviews can also help auditors understand what is being heard by employees, which might be very different than the message that management thinks it is delivering. Again, this information can be very useful in identifying and correcting situations where unethical or illegal conduct might be likely to occur.

Separately, the Guidelines require that the organization ensure that employees and agents have effective mechanisms available through which they may report potential or actual misconduct anonymously or confidentially, and that any individuals who come forward are protected against retaliation for such reports. These mechanism must also be available to those seeking guidance about ethical or compliance issues, not just those who have complaints. It should be noted that confidential or anonymous internal reporting mechanisms are meant to supplement, not replace, the normal lines of communication within a company.[28]

Importantly, an effective internal reporting mechanism must include procedures to investigate, track, and follow-up on concerns and, where necessary, to take action to correct, mitigate and prevent potential misconduct. *See supra* Part II.B.7 (discussing the Guidelines' specific requirements for corrective action.) Failure to quickly investigate and resolve concerns can decrease the credibility of the compliance program and morale and can allow small problems to quickly escalate into legal, economic and reputational crises. It is particularly important to have trained internal investigators to respond to complaints or concerns, combined with a mechanism to alert counsel when it is necessary to conduct a privileged investigation or, in the case of serious matters, engage outside counsel to conduct investigations.

The investigation and tracking procedures should apply to all complaints and concerns that are raised, whether they are made directly to supervisors or through the "hotline." Companies that formally track only "hotline" calls may not realize that they are leaving out considerable volumes of data because more complaints were made to supervisors than through the "hotline."

**It is particularly important to have trained internal investigators to respond to complaints or concerns.**

An effective and credible internal reporting mechanism must be well-publicized and easy to use. Otherwise, it will create the impression that the company does not really want to receive complaints or questions. Simply putting information about the program on the company intranet usually is not sufficient. Posters, training, and other means of regularly reminding employees and agents about how to raise questions or concerns is recommended. Even the program's name should be carefully thought through: "hotline," "helpline," "whistleblower line," and "ethics line" all convey slightly different messages.

**6. Discipline and Incentives**

According to the Guidelines, "[t]he organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct."[29]

The Guidelines requirement of "incentives" for personnel to perform in accordance with the company's compliance program is a somewhat controversial provision, as some commentators believe that it sends the wrong message to reward individuals for good conduct (implying that good conduct is above and beyond what is expected), while others believe that this is an important positive message that should be used to counterbalance purely "negative incentives" (*i.e.*, punishment), and to demonstrate that good conduct, not simply financial performance, will be rewarded. Regardless, the Guidelines are clear that incentives are necessary under an effective program. Care must also be taken to avoid creating incentives to not report problems (*e.g.*, where reporting misconduct in one's department might create a "negative hit" on one's bonus).

The Guidelines also direct that the compliance program be consistently enforced, and that appropriate disciplinary measures be taken when someone engages in illegal conduct. This is very important to the credibility of the program: if individuals who violate the law or company policy are not disciplined, that sends the message that management does not really take compliance and ethics seriously. This can become particularly problematic when a stellar performer from a financial perspective is perceived by his or her colleagues as "getting away with" violations of company policy. The fail-

[28] Multinational retailers that operate in the EU must ensure compliance with local employment and data protection laws in implementing an internal reporting system. *See* Schreiber, et al., *Anonymous Sarbanes-Oxley Hotlines for Multi-National Companies: Compliance with E.U. Data Protection Laws*, The Practitioner's Guide to the Sarbanes-Oxley Act, Vol. II, American Bar Assoc. (2006) for a more comprehensive discussion.

[29] *Guidelines* § 8B2.1(b)(6).

ure to impose discipline is also an important signal to regulators and enforcers about management's commitment to compliance. If a bad actor is getting bonuses, it makes it more difficult to argue that the individual was really acting outside of company policy.

The Guidelines expand the scope of discipline beyond those who engage in the actual misconduct to those who fail to take reasonable steps to prevent or detect misconduct. In other words, a manager who ''looks the other way'' or who fails to implement the compliance program's measures to detect misconduct should be subject to discipline.

It is important that both discipline and incentives be consistently applied. Failure to do so can have a number of negative impacts, ranging from decreased morale to allegations of discriminatory practices. Consistent application throughout the organization is key.

### 7. Corrective Action: Reasonable Steps to Respond to Misconduct

Finally, the Guidelines require that compliance programs adopt certain procedures to address misconduct after it occurs. ''After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.''[30] The 2010 amendments add a commentary note explaining that the ''reasonable steps'' an organization should take to remedy the harm caused by misconduct ''may include . . . providing restitution to identifiable victims, . . . self reporting and cooperation with authorities.''[31] In addition, the note explains that organizations must ''act appropriately to prevent further similar criminal conduct,'' including through assessments of the ''compliance and ethics program'' and ''modifications necessary to ensure the program is effective.''[32] In other words, organizations must assess why the misconduct occurred and how to prevent it in the future, and then modify the program accordingly.

As a consequence, an organization's auditing procedures must be accompanied by corrective and preventive action procedures that determine the cause of any detected shortcomings, correct and mitigate the consequences of such problems, and identify the actions necessary to prevent their recurrence (including changes to the compliance program). These corrective and preventive action procedures should be triggered by detections of non-compliant or unethical conduct from any source, not just auditing. Government investigators pay close attention to the corrective action process. It is very difficult to credibly explain away a detected but uncorrected problem. Indeed, knowingly allowing misconduct to continue can be the trigger for a serious criminal investigation.

It is also important to have defined processes for internal and external reporting. The Board (or the Auditing Committee) and senior management should receive regular reports on audit results and the status of corrective action. As has been well-publicized in the recent corporate scandals, the government is not receptive to the ''I did not know'' defense by senior managers. The Board and senior management need to know how the ethics and compliance program is performing, including information such as the results of audits, the status of corrective action, summaries of hotline reports, etc. This information should be presented in a meaningful way such that the key points and trends are identified and appropriate actions can be taken. For example, simply electronically copying senior management on detailed audit reports is usually not effective. The Board (or Auditing Committee) has a particularly important oversight role where there is a possibility that senior management might be implicated (including separately retaining counsel to conduct independent investigations, if necessary).

Practices regarding required or prudential reporting to the authorities should also be developed. Failure to comply with mandatory reporting requirements can have very serious consequences. Even where there are no mandatory reporting requirements, regulators, enforcers and courts often take a company's voluntary disclosures and cooperation into account in determining what, if any, enforcement response is appropriate.

## C. Risk Assessment

In addition to following the seven necessary steps just explained, the Guidelines provide that ''[t]he organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each [of the seven above mentioned] requirement[s] . . . to reduce the risk of criminal conduct identified through this process.''[33]

In the commentary, the Commission states that organizations will have to assess the nature and seriousness of potential violations of the law, the likelihood that certain violations of the law may occur because of the nature of the organization's business, and the prior history of the organization. Assessments of legal risk are not a one-time event: they must be conducted on an ongoing or periodic basis so that the assessment is kept current and violations of the law are prevented.

The design and implementation of compliance programs must take into account the risks identified in the assessment. The commentary to the Guidelines provides examples on how this is expected to work. For example, retailers and other organizations that employ sales personnel who have flexibility to set prices ''shall establish compliance standards and procedures designed to prevent and detect price fixing,'' while organizations whose sales employees have the flexibility to ''represent the material characteristics of a product shall establish compliance standards and procedures to prevent fraud.''[34]

There is as yet no consensus on what constitutes the ''best practice'' for conducting risk assessments. At one end of the scale are extremely detailed and quasi-quantitative assessments, while at the other end, some companies identify their primary legal challenges in relatively broad strokes. The prudent practice is a thorough enough review so that the Board and senior management will understand what the legal risks are at a sufficient level of detail to understand what must be done to effectively manage them. This should include the risk of civil, not just criminal violations, as significant liabilities may arise from civil violations and the

[30] *Id.* § 8B2.1(b)(7).
[31] *Id.* § 8B2.1(b), cmt. 6.
[32] *Id.*

[33] § 8B2.1(c).
[34] *Id.* § 8B2.1, cmt. 7.

   ISSN 0148-8155

line between civil and criminal liability is becoming increasingly blurred. There is no requirement in the Guidelines for complex quantitative assessments or ranking systems; indeed, in some situations, such approaches may be unnecessarily expensive and cumbersome and not provide significant marginal value.

No matter what approach is adopted, it is prudent to involve counsel in this process, not solely for the purpose of cloaking the inquiry in attorney-client privilege (although there may be instances where this is a good idea), but because lawyers have professional expertise in evaluating the applicability of legal requirements and understanding the likelihood and risks of non-compliance. Relying solely on non-lawyers to identify applicable legal requirements and assess the likelihood of non-compliance can produce an inadequate or even inaccurate assessment.

## III. Using Effective Compliance Programs to Reduce or Eliminate Criminal Penalties

If a corporation finds itself under investigation by federal prosecutors or regulators, having an effective compliance program in place can provide an invaluable tool. The Guidelines' emphasis on the importance of effective compliance programs is clear, but the true effect of having such a program can be difficult to measure in concrete terms. The primary reason for this is that very few criminal prosecutions against corporate defendants proceed through the traditional criminal justice system. Instead, prosecutors and corporations alike increasingly favor deferred prosecution agreements, non-prosecution agreements, or other administrative/civil settlements. These agreements eliminate the risks and costs of litigation for both parties and thus can be mutually beneficial in some cases. However, because they do not result in a conviction and sentence, they do not require application of the Guidelines. As a consequence, only a handful of examples exist in which a convicted corporate defendant received credit at sentencing due to an effective compliance program.[35]

Yet examining actual sentences alone vastly understates the critical importance of an effective compliance program. An effective program can be instrumental in limiting the government's response in the event misconduct occurs and is reported to the government or otherwise comes to the government's attention. Indeed, ''with the exception of the Antitrust division, the [DOJ] now recognizes as a matter of policy that an [effective compliance program] should be a factor in deciding whether or not DOJ will file criminal charges in cases of organizational misconduct.''[36]

**Any retailer with a compliance program that meets the Guidelines' core requirements has made critical strides towards preventing the risk of corporate liability and, to the extent it happens, minimizing its impact.**

Moreover, DOJ policies require prosecutors to consider the existence of a ''pre-existing compliance program'' in deciding whether to enter into a deferred or non-prosecution agreement.[37] As a result, DOJ frequently asks for information about a company's compliance program when conducting civil and criminal investigations.

The effectiveness and credibility of these programs can be an important factor in determining the government's enforcement response, and can result in a favorable settlement or, in some cases, a government decision not to pursue enforcement at all.

A greater challenge for retailers can be tailoring a compliance program to fit the standards of the numerous federal agencies that regulate the retailer's multiple business lines. Each agency—and even individual divisions within larger agencies such as the DOJ—have somewhat different views of the ideal compliance program. Yet the seven elements described above provide an essential foundation. Any retailer that can develop a compliance program that meets the Guidelines' core requirements has made critical strides towards obtaining a program that will prevent the risk of corporate liability and, to the extent it happens, minimize its impact. With the assistance of experts, refinements can be made to tailor the compliance program to the specific regulatory regimes to which the individual retailer is subject.

## IV. Conclusion

All retailers with significant business operations in the United States should endeavor to adopt a compliance and ethics program based on the template the Guidelines provide. While the likelihood of federal criminal prosecution may be small, the results of a prosecution can be catastrophic, and creating an effective compliance program helps substantially to prevent those risks and, to the extent they occur, minimize their impact.

An effective compliance program provides management timely and accurate information about potential problems and issues, which has a dramatic effect on outcomes from both an enterprise risk management and business perspective. In addition, DOJ has developed policies that take into account an organization's compliance assurance systems in determining whether and how to respond to non-compliance. Further, the program will be helpful at the sentencing phase if it ever comes to that. Applying the practical advice provided in this article will enable a company to demon-

[35] Indeed, from 1991 to 2011, the U.S. Sentencing Commission reported that only five convicted corporate defendants received a reduced sentence because of an effective compliance program. ERC Report, *supra* n. 1, at 37.

[36] *Id.* at 2-3. This DOJ policy has been memorialized in two memoranda. See *Principles of Federal Prosecution of Business Organizations* (U.S. DOJ, December 12, 2006, known as the ''*McNulty Memo*,'' which superseded the January 20, 2003 ''*Thompson Memo*''); *Federal Prosecution of Corporations* (U.S. DOJ, June 16, 1999). The Securities and Exchange Commission has adopted a substantially similar policy. See SEC Accounting and Auditing Enforcement Release No. 1470 (October 23, 2001), known as the ''*Seabord Report*.''

[37] U.S. Attorneys' Manual §§ 9-28.300, 9-28.800 http:/www.justice.gov/usao/eousa/foia_reading_room/usam/.

strate that its compliance program is effective under the Guidelines.

  DER ISSN 0148-8155