CHAPTER 13

CORPORATE COMPLIANCE PROGRAMS

Benjamin Gruenstein[*]

SYNOPSIS

---

[*] Portions of this Chapter were carried over from the work of Jay M. Cohen, who authored the Chapter until 2015.

§ 13.01 Introduction to Corporate Compliance Programs

Companies face increasing demands from regulators, legislators and their shareholders to strengthen their organizational ethics and compliance programs. With each new scandal, proscriptions and expectations have intensified and spread from specific industries to the broader economy. Earlier this century, mandates in the Sarbanes-Oxley Act of 2002[1] (the "Sarbanes-Oxley Act" or "Sarbanes-Oxley") and related regulations made an effective compliance program with a strong code of conduct a required element of every public company's overall program for communicating and fulfilling its commitment to ethics, integrity, and compliance with laws and regulations. Since then, prosecutors and regulators have made clear that, in deciding whether and on what terms to settle securities fraud and other cases, they will consider whether companies have instituted an effective compliance program.

In this chapter, we will analyze the legal, regulatory and "best practice" requirements for compliance programs and offer some practical advice on how to best implement them.

We also will review several decades of efforts, in particular by the U.S. Department of Justice ("DOJ") and the Securities and Exchange Commission ("SEC"), to develop, implement, and enhance standards for organizational compliance programs. These initiatives are worth examining for several reasons.

First, these efforts have defined the substance and goals of organizational compliance programs. In the process, they have contributed to the widespread recognition of the code of conduct as an indispensable means of promoting organizational integrity.

Second, these initiatives offer a large body of information regarding what works in the design, implementation and enforcement of organizational compliance programs. This practical experience can assist organizations in meeting regulatory mandates and stakeholder expectations, and in ensuring that their programs have a demonstrable, positive impact on organizational behavior.

This is a critical point for compliance officers and corporate counsel considering how best to develop or improve their organizations' compliance program. After all, a number

[1] The Sarbanes-Oxley Act, Pub. L. No. 107-204, 116 Stat. 745 (July 30, 2002) (codified in scattered sections of 11 U.S.C.; 15 U.S.C.; 18 U.S.C.; 28 U.S.C.; and 29 U.S.C).

of companies caught up in scandals and misconduct had some aspects of a compliance program, but not enough to keep them out of trouble. For example, the Enron Board of Directors approved three separate waivers of the conflicts of interest provisions in its code of conduct when it allowed the chief financial officer to have large, personal financial interests in entities doing business with the company and then to profit at the company's expense. As summarized by the report of an investigative committee of the United States Senate, "the Enron Board's decision to waive the company's code of conduct and allow its Chief Financial Officer ("CFO") to establish and operate off-the-books entities designed to transact business with Enron was also highly unusual and disturbing." The refusal to enforce the code of conduct contributed to the collapse of the company and the defrauding of shareholders, because "hundreds of millions of dollars that should have stayed with Enron shareholders instead lined the pockets" of the CFO and other investors in these entities.[2] More recently, questions have been raised about alleged contradictions between the actions of financial services companies and their employees, and the commitments to integrity and transparency—to putting customers first and avoiding conflicts of interest—found in the compliance policies for these organizations.

It is not sufficient to have a code of conduct on paper, even one that on its face hits all of the key points, if that code is not understood, respected and followed, from the top of the organization on down. The DOJ has consistently and repeatedly stressed that it will not credit the compliance programs of companies that have "merely a 'paper program' " that is not "designed and implemented in an effective manner."[3] Employees must believe that the code will be applied consistently and fairly, they must expect that everyone in the organization will be held to its standards and they must trust that their employer will keep its promise not to tolerate any retaliation for good faith reports of possible misconduct. The practical information we will review can help organizations ensure that their codes receive the required attention and respect.

One court has refused to dismiss an allegation that a financial services company made material misrepresentations to shareholders and the public when the organization's actions failed to meet the standards in its publicly disseminated code of conduct. According to the court, the company failed to meet the "rules and ethical principles that governed [it] . . . If [the company's] claims of 'honesty' and 'integrity' are simply puffery, the world of finance may be in more trouble than we recognize."[4] Most companies proudly, and publicly, proclaim their commitment to ethics, integrity and

---

[2] *See* The Role of the Board of Directors in Enron's Collapse, S. Rep. No. 107-70 (2002), at 24, 38.

[3] P. McNulty, Principles of Federal Prosecution of Business Organizations, at 14 (Jul. 5, 2007) ("McNulty Memo"), *available at* https://www.justice.gov/sites/default/files/dag/legacy/2007/07/05/mcnulty_memo.pdf. *See also* Leslie R. Caldwell, Remarks by Assistant Attorney General for the Criminal Division Leslie R. Caldwell at the 22nd Annual Ethics and Compliance Conference (Oct. 1, 2014), *available at* https://www.justice.gov/opa/speech/remarks-assistant-attorney-general-criminal-division-leslie-r-caldwell-22nd-annual-ethics ("And as important as the compliance program itself is implementation . . . . More than just reading the paper program or the code of conduct, we look at what employees are told in their day to day work.").

[4] *See* Richman v. Goldman Sachs Group, Inc., F. Supp. 2d 261 (S.D.N.Y 2012).

putting customers first. The right compliance program, accompanied by a serious code of conduct, will help them mean what they say.

Third, it is important to examine the history of compliance programs because regulators, prosecutors and courts have articulated their expectations for such programs, as well as the possible advantages to organizations of having an effective program. These expectations and advantages continue to this day and, if anything, have grown as the result of the regulatory responses to the many scandals of this millennium.

Fourth, the regulatory and practical development of organizational compliance programs must be placed in the context of another element that has emerged as significant: the focus on the organization's "culture of compliance" in addition to its compliance structure and process. We will examine what it means to have such a culture, according to regulators and experts; how to promote and encourage this culture; why it is an asset to any organization; and some ways of determining if efforts to build this culture are succeeding.

For any organization to succeed in this challenging environment, it is essential to have a compliance program that is comprehensive, realistic and consistently enforced. Corporations can manage compliance on their own terms or, as companies that run afoul of regulations and regulators continue to learn, be forced to strengthen their compliance programs and controls as part of a costly settlement and while subject to the supervision of the government or an independent compliance monitor.[5]

Organizational compliance programs are designed to accomplish two fundamental goals. First, they seek to prevent, detect and appropriately respond to violations of laws, regulations and company policies and, in the process, to promote ethical behavior within the organization. In so doing, these programs strive to lessen the likelihood that the organization or its individual employees will fail to meet legal and regulatory obligations and commitments to customers, fellow employees, shareholders and other stakeholders. Compliance programs accomplish this by making sure that employees know what these obligations and commitments are and by giving them avenues (such as confidential hotlines) to ask questions or report concerns. These programs also can minimize adverse consequences and prevent small problems from becoming more serious ones, by identifying and detecting problems quickly.

Second, a carefully organized and consistently enforced compliance program can enable a company to limit or even avoid corporate liability for the compliance failures of individual employees. A corporate compliance program will not necessarily "immunize the corporation from liability when its employees, acting within the scope of their authority, fail to comply with the law."[6] Organizations remain responsible for

---

[5] *See, e.g.*, Press Release, U.S. Dep't of Justice, Odebrecht and Braksem Plead Guilty and Agree to Pay at Least $3.5 Billion in Global Penalties to Resolve Largest Foreign Bribery Case in History (Dec. 21, 2016), *available at* https://www.justice.gov/opa/pr/odebrecht-and-braskem-plead-guilty-and-agree-pay-least-35-billion-global-penalties-resolve.

[6] United States v. Twentieth Century Fox Film Corp., 882 F.2d 656, 660 (2d. Cir. 1989).

the misdeeds of their employees.[7] Nevertheless, even if it does not stop every instance of corporate wrongdoing by errant employees, a well-designed and consistently enforced compliance program can make the organization less culpable in the eyes of regulators and prosecutors.

A code of conduct contributes to the objectives of organizational compliance programs by emphasizing senior management's commitment to compliance and then informing employees about the organization's fundamental principles and values; its key compliance issues, regulations and standards; the resources available to help employees understand and meet these values and standards; and the means of monitoring and enforcing them.

§ 13.02 Legal and Regulatory Background

[1] DOJ

[a] Federal Sentencing Guidelines for Organizations

[i] *Development of the FSGO*

The federal sentencing guidelines for organizations ("FSGO") were the single most influential step in the evolution of corporate compliance programs.

In the five years before the adoption of the FSGO, many voices urged more widespread adoption of corporate compliance programs. As one relevant example, the Treadway Commission, which examined fraudulent financial reporting well before the 21st century financial scandals, recommended that every public company have a code of conduct:

> Public companies should develop and enforce written codes of corporate conduct. Codes of conduct should foster a strong ethical climate and open channels of communication to help protect against fraudulent financial reporting. As part of its ongoing oversight of the effectiveness of internal controls, a company's audit committee should review annually the program that management establishes to monitor compliance with the code.[1]

The FSGO subsequently gave companies a very good reason to follow that advice. These guidelines were developed as part of a congressionally mandated reform of federal sentencing that began with the creation and appointment of the United States Sentencing Commission (the "Sentencing Commission") in 1984.[2] The Sentencing Commission, a permanent body of three judges and four other persons appointed by the President and confirmed by the Senate, was given the responsibility to create rules that would reduce the vast sentencing discretion then given to federal judges. In 1987, the Sentencing Commission issued the first binding sentencing guidelines applicable to individual defendants. The guidelines created ranges for each sentence, based on the "offense level" for the particular crime and the offender's "criminal history" score.

---

[7] *See* United States v. Ionia Management, S.A., 555 F.3d 303 (2d Cir. 2009).

[1] *See* Report of the National Commission on Fraudulent Financial Reporting (1987), at 35, *available at* www.coso.org.

[2] The Sentencing Reform Act of 1984, Pub. L. No. 98-473, 98 Stat. 1987.

The Sentencing Commission next focused on the adoption of guidelines for the sentencing of organizations convicted of federal crimes.

[ii] ***Purpose and Structure—The "Carrot and Stick"***

After three years of study and public comment, the FSGO were adopted as Chapter Eight of the sentencing guidelines and became effective on November 1, 1991.[3] They contain a similar system of sentencing ranges, this time using two criteria: a "base fine" that reflects the seriousness of the offense and a "culpability score" for the offending organization. Taken together, these factors define a range of possible fines for the sentencing court to use in determining the penalty imposed on an organization in each case. In addition to being fined, organizations can be placed on probation and ordered to make restitution and other payments.

Like its efforts with the sentencing guidelines for individuals, the Sentencing Commission sought through the FSGO to reduce variations in the sentencing of organizations by limiting the discretion of federal judges. But the Sentencing Commission hoped to influence organizational behavior in more fundamental ways.[4]

First, the FSGO are not limited to corporations. Instead, they apply to "any organization," including "corporations, partnerships, associations, joint-stock companies, unions, trusts, pension funds, unincorporated associations, government and political subdivisions thereof, and non-profit organizations."[5]

Second, the guideline ranges for organizations generally result in much stiffer fines being imposed than was the case under the prior system. The Sentencing Commission was concerned that the "unpredictability and variation in the sanctions imposed on convicted corporations meant that there was no obvious incentive to galvanize resources to avoid such sanctions." Fines were inconsistently imposed, or "less expensive than avoiding liability in the first place."[6]

Third, and most important, the Sentencing Commission expressly adopted what many commentators have called a "carrot and stick" approach to the sentencing of organizations, one that offers a tangible benefit to organizations with effective compliance programs. The key for our purposes is that an organization's culpability score generally will be determined by (i) the steps taken by the organization prior to the offense to prevent and detect criminal conduct, (ii) the level and extent of the involvement in or tolerance of the offense by senior management or the board of directors, and (iii) the organization's actions after the offense has been committed.[7]

---

[3] U.S. Sentencing Guidelines Manual, Ch.8 (Nov. 2002) [hereinafter "1991 USSG" or the "1991 Guidelines Manual"].

[4] *See* Nagel, I. & Swenson, W. M., *The Federal Sentencing Guidelines for Corporations: Their Development, Theoretical Underpinnings, and Some Thoughts About Their Future*, 71 WASH. U.L.Q. 205, 214–217 (1993).

[5] 1991 USSG § 8A1.1, Application Note 1.

[6] *See* Report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines (Oct. 7, 2003) [hereinafter Ad Hoc Advisory Group Report], at 12.

[7] 1991 USSG, Ch. 8, Introductory Commentary.

As noted by the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines (the "Ad Hoc Advisory Group"), which was appointed by the Sentencing Commission in February 2002 to review and suggest changes in the FSGO:

> The centerpiece of the [FSGO] is the fine range, from which a sentencing court selects the precise fine to impose on a convicted organization . . . Guidelines provide for substantial fines when a convicted organization has encouraged, or has been indifferent to, violations of the law by its employees, but impose significantly lower fines when a corporation has demonstrated in specified ways its antipathy toward lawbreaking.[8]

In fact, organizations that self-report, fully cooperate and accept responsibility can significantly reduce their culpability score, and thus in some circumstances reduce their maximum fine by as much as 90%. This can translate into savings of millions of dollars, if they have taken the steps outlined below, including the adoption of an effective compliance program. This "carrot and stick" approach remains in the guidelines today, even after recent changes in the specific steps that organizations must take to earn this credit.

One reason that the Sentencing Commission chose this approach was to address, albeit in an indirect way, standards of organizational criminal liability that were (and remain), as one expert explains, "indifferent to the culpability of the organization—as opposed to those agents within the organization—for the criminal acts." Criminal liability can attach to an organization based on the conduct of its employees or agents, *even when that conduct is contrary to company policy*:

> The imputed culpability liability theory fails to distinguish between offenses committed with the participation or encouragement of upper management, pursuant to corporate policies or procedures, and those committed by "rogue employees" whose acts violated company policy or could not have been prevented by careful supervision.[9]

The Sentencing Commission wanted to address this issue by distinguishing those organizations trying to prevent wrongdoing from those which did not, and at least giving the former meaningful credit at sentencing for their efforts.

The Sentencing Commission's goals—reflected in its "carrot and stick" approach—were even more ambitious than that. As noted in the report of the Ad Hoc Advisory Group, the Sentencing Commission wanted not only to define the punishment for convicted organizations but also to affect organizational behavior outside the courtroom. The idea was to create a sentencing system that encourages organizations to prevent crime in the first instance, and to detect and disclose offenses more often and much sooner when they do occur. The Sentencing Commission "structured its framework to create a model for the good 'corporate' citizen; use the model to make organizational sentencing fair and predicable; and ultimately employ the model to create incentives for organizations to deter crime."[10] It is because of these incentives that the impact of the FSGO on organizational governance and compliance activities has been so profound.

---

[8] Ad Hoc Advisory Group Report at 20.

[9] Jennifer Moore, *Corporate Liability Under the Federal Sentencing Guidelines*, 34 ARIZ. L. REV. 743.759 (1992).

[10] Ad Hoc Advisory Group Report at 14.

[iii] *Definition of an "Effective" Compliance Program in the 1991 Guidelines*

The Sentencing Commission's "carrot and stick" approach was codified in the 1991 FSGO in several related provisions. An organization's culpability score—and thus the penalty that it faced—could be substantially reduced if "the offense occurred despite an effective program to prevent and detect violations of law."[11] The FSGO defined an "effective program" as one "that has been reasonably designed, implemented, and enforced so that it generally will be effective in preventing and detecting criminal conduct." To meet this standard, an organization was obligated to exercise "due diligence in seeking to prevent and detect criminal conduct by its employees and other agents."[12]

This due diligence required "at a minimum" that the organization takes seven steps, including the establishment of compliance policies and procedures such as a code of conduct; compliance background reviews of key personnel; compliance communications and training; monitoring and auditing of business unit compliance with the policies and procedures; consistent enforcement and discipline; appropriate responses to compliance problems; and assignment of compliance responsibility and oversight to "specific individual(s) within high-level personnel of the organization."[13]

In addition to the credit that an organization could get for taking these steps, it could reduce its culpability score by reporting the offense to the government, cooperating with any investigation into the matter and accepting responsibility for the crime.[14]

The FSGO further provided that the structure and shape of each organization's compliance program should depend on the size of the organization, the "likelihood that certain offenses may occur" because of the nature of its business and its prior history, including any previous offenses. Indeed, "an organization's failure to incorporate and follow applicable industry practice or the standards called for by any applicable governmental regulation weighs against a finding of an effective program to prevent and detect violations of law."[15] Moreover, even organizations with compliance programs could be denied sentencing credit if "high-level personnel . . . or an individual responsible for the administration or enforcement of [the] program . . . participated in, condoned, or was willfully ignorant of the offense."[16]

The original FSGO have served as the foundation for three decades of organizational compliance efforts, and they continue to influence and be reflected in judicial criteria, regulatory expectations and compliance "best practices."

---

[11] 1991 USSG § 8C2.5(f) ("Effective program to Prevent and Detect Violations of Law").

[12] 1991 USSG § 8A1.2, Application Note 3(k).

[13] 1991 USSG § 8A1.2, Application Note 3(k).

[14] 1991 USSG § 8C2.5(g) ("Self-Reporting, Cooperation, and Acceptance of Responsibility").

[15] 1991 USSG § 8A1.2 Application Note 3(k).

[16] 1991 USSG § 8C2.5(f).

[iv] *The 2004 Amendments to the FSGO*

The elements of the FSGO related to compliance programs were not altered from their inception in 1991 until November 2004. As discussed above, in February 2002, the Sentencing Commission appointed the Ad Hoc Advisory Group to review and evaluate the effectiveness of the guidelines, with "particular emphasis on examining the criteria for an effective program to ensure an organization's compliance with the law."[17] The Ad Hoc Advisory Group decided at the outset that the "widespread misconduct in some of the nation's largest publicly held companies . . . required evaluation of whether the compliance efforts precipitated by the organizational sentencing guidelines could be made more effective in preventing and detecting violations of law."[18] It then spent 18 months studying the evolution and impact of organizational compliance programs in the period since the adoption of the FSGO.

The conclusions of the group are reflected in its report to the Sentencing Commission on October 7, 2003. The Ad Hoc Advisory Group recommended that the Sentencing Commission create a standalone guideline defining an "effective" compliance program, in order to highlight the importance of these provisions.[19] The compliance program definition was, at the time, part of the "Commentary to United States Sentencing Guidelines § 8A1.2 (Application Instructions-Organizations)" in Chapter Eight of the sentencing guidelines.

The group also reiterated the basic elements of the existing FSGO, but at the same time proposed substantive changes to the seven elements, including amendments that would mandate, rather than suggest, the steps that organizations must take to qualify for this credit. These changes were designed to create more rigorous standards for evaluating organizational compliance programs.

In another significant development, the Ad Hoc Advisory Group recommended that the Guidelines spell out the responsibilities of an organization's governing authority and organizational leadership for compliance efforts and the compliance culture.[20] Finally, the changes sought to extend compliance efforts beyond mere compliance with written legal standards to the development of "an organizational culture that encourages a commitment to compliance." This emphasis on culture and leadership is likewise reflected in the rules for codes of conduct that were developed in 2003 by the SEC and the stock exchanges after Sarbanes-Oxley. In each of these efforts, the code of conduct became an even more central part of an effective compliance program.

On April 30, 2004, the Sentencing Commission submitted its final proposal to Congress, largely adopting the recommendations of the Ad Hoc Advisory Group,

---

[17] *See* News Release, The Sentencing Commission Convenes Organizational Guidelines Ad Hoc Advisory Group (Feb. 21, 2002), *available at* https://www.ussc.gov/about/news/press-releases/february-21-2002. This action by the Sentencing Commission would later help it to meet the mandate in Sarbanes-Oxley Act Section 805(a)(2)(5) that it determine if the FSGO are "sufficient to deter and punish organizational criminal misconduct."

[18] Ad Hoc Advisory Group Report at 3.

[19] Ad Hoc Advisory Group Report at 4.

[20] Ad Hoc Advisory Group Report at 4–5.

including the recommendation to create a standalone guideline.[21] The Commission's proposed changes to the FSGO took effect on November 1, 2004, without any further modifications by Congress.[22] This created a new standard against which organizational compliance programs are now evaluated.

The amended FSGO continue to reflect many of the same elements of an "effective" compliance program that were central to the 1991 guidelines. For example, the amended guidelines continue to require that organizations (1) "establish standards and procedures to prevent and detect criminal conduct," (2) use reasonable efforts not to employ in key positions "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," and (3) respond appropriately and effectively to criminal conduct.[23]

At the same time, the 2004 FSGO amendments make three significant changes to the original guidelines.

First, the 2004 amendments have made mandatory certain elements that were simply encouraged in the prior version. For the first time they provide that:

(1) Organizations must conduct "effective training programs" and otherwise disseminate information about their compliance and ethics programs.[24]

(2) Organizations must include "monitoring and auditing" in their efforts to ensure that the compliance and ethics program "is followed."[25]

(3) Organizations "shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify" their programs to reduce that risk. These risk assessments must be customized to reflect the specific issues and concerns faced by the organization based on its industry, size and structure, and compliance history.[26]

(4) Organizations must "have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation."[27]

(5) The compliance and ethics program must be "promoted and consistently

---

[21] *See* Amendments to the Sentencing Guidelines, Policy Statements, and Official Commentary (May 1, 2004), *available at* https://www.ussc.gov/guidelines/amendments/reader-friendly-version-2004-guideline-amendments-sent-congress.

[22] The amended FSGO (as set forth in the 2004 Federal Sentencing Guidelines Manual, Chapter 8 "Sentencing of Organizations") are available at https://www.ussc.gov/guidelines/archive/2004-federal-sentencing-guidelines-manual. Hereinafter, citations to sections of the 2004 FSGO are to "2004 USSG."

[23] 2004 USSG §§ 8B2.1(b)(1), (3) and (7).

[24] 2004 USSG § 8B2.1(b)(4)(A).

[25] 2004 USSG § 8B2.1(b)(5)(A).

[26] 2004 USSG § 8B2.1(c).

[27] 2004 USSG § 8B2.1(b)(5)(C).

enforced" through both "appropriate incentives" and "appropriate disciplinary measures."[28]

Second, as recommended by the Ad Hoc Advisory Group, the 2004 FSGO amendments added specific references to the responsibilities of the board of directors and senior management:

(1) "The organization's governing authority [its Board of Directors] shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight" of the implementation and effectiveness of the program.[29]

(2) Senior leaders of the organization must ensure that it has an effective compliance and ethics program, as defined by the guidelines.[30]

(3) Senior leaders and the board must also receive periodic reports about the effectiveness of the compliance and ethics program, from the individuals with operational responsibility for the program.[31]

(4) The individual responsible for the compliance and ethics program must be given "adequate resources, appropriate authority, and direct access" to the organization's board of directors. The Sentencing Commission also noted that "a large organization shall devote more formal operations and greater resources in meeting the requirements of this guideline than shall a small organization."[32]

Third, and perhaps most significant, the 2004 amendments to the FSGO added an entirely new element to the definition of an "effective" compliance program. For the first time, they required organizations to "promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law." This simple, straightforward emphasis on culture, in addition to process introduced a more demanding element into the equation and has broadened the impact of the FSGO on organizational leadership and conduct. This impact is reflected in the comments and expectations of regulators, especially the SEC, which we will explore in more detail later in this chapter.

Like the 1991 guidelines, the amended FSGO also provide that, in addition to having an effective compliance and ethics program, organizations can get credit at sentencing for "self-reporting, cooperation and acceptance of responsibility."[33] In fact, the "Introductory Commentary" that accompanies the revised guidelines in Chapter Eight of the Guidelines Manual states that "[t]he two factors that mitigate the ultimate punishment of an organization are: (i) the existence of an effective compliance and

---

[28] 2004 USSG § 8B2.1(b)(6).

[29] 2004 USSG § 8B2.1(b)(2)(A).

[30] 2004 USSG § 8B2.1(b)(2)(B).

[31] 2004 USSG § 8B2.1(b)(2)(C).

[32] *See* 2004 USSG § 8B2.1 Application Note 2(C)(ii).

[33] 2004 USSG § 8C2.5(g).

ethics program; and (ii) self-reporting, cooperation, or acceptance of responsibility." This latter factor, as we shall see below, has become increasingly important to regulators and prosecutors.

One change in 2004 proved especially controversial and was later reversed by the Sentencing Commission, in response to complaints from the Association of Corporate Counsel, the United States Chamber of Commerce and other interested parties. The Sentencing Commission sought to address the growing concern that organizations were being "pressured" by prosecutors to waive their attorney-client privilege and work-product protections in order to demonstrate the kind of cooperation contemplated by the FSGO. New commentary to this section explained that "[w]aiver of attorney-client privilege and of work product protections is not a prerequisite to a reduction in culpability score [under these provisions] unless such a waiver is necessary in order to provide timely and thorough disclosure of all pertinent information known to the organization."[34] The goal was to make waiver requests *less* likely, but many in the legal community viewed the language quite differently. A group of former U.S. Attorneys General wrote in August 2005 that this commentary—rather than encourage a case-by-case consideration of the issue—has instead been interpreted by prosecutors as providing "[c]ongressional ratification of the Department [of Justice's] policy of routinely asking that privilege be waived."[35] The National Association of Criminal Defense Lawyers ("NACDL") called this "probably one of the most important issues, post-Enron, facing the white-collar criminal defense bar."[36] The Commission subsequently received public comment and held two hearings just on this issue. On May 1, 2006, the Commission submitted to Congress proposed changes in the FSGO, including a recommendation to eliminate the language regarding waiver of the attorney-client privilege and work-product protections. On November 1, 2006, this change became effective in the absence of action by Congress. The battle over waivers by organizations of the attorney-client privilege is still being waged on other fronts, as discussed later in this chapter.

On January 12, 2005, the United States Supreme Court ruled that the federal sentencing guidelines must be treated as only advisory, not mandatory.[37] This means that judges must still consider the guidelines when imposing sentences on individual or corporate defendants but are not obligated to apply them in each case. Nonetheless, an organization finding itself in front of a federal judge for sentencing should want to demonstrate its commitment to compliance, ethics and self-policing, as evidenced by its faithful and effective adherence to the principles and elements of the FSGO. More important, the use of the FSGO as the standard by which organizations are judged—and the impact of the FSGO outside the courtroom—remain as real as ever, for the reasons discussed below.

---

[34] 2004 USSG § 8C2.5 Application Note 12.

[35] *See* Waiving privilege a crucial sentencing issue, NATIONAL LAW JOURNAL, Aug. 29, 2005, at 6.

[36] *Id.*

[37] United States v. Booker, 543 U.S. 220 (2005).

[v] *The 2010 Amendments to the FSGO*

On November 1, 2010, several additional changes to the FSGO took effect. For purposes of this discussion, the most significant amendment provides that, for the first time, companies can win sentencing credit for having an effective compliance program, even when senior executives and other "high-level personnel" were involved in, condoned or were "willfully ignorant" of the misconduct, if:

(1) The compliance program detected the offense before anyone outside the organization discovered or was reasonably likely to discover it;

(2) The company promptly reported the offense to the authorities;

(3) Nobody in charge of the ethics and compliance program participated in, condoned or willfully ignored the misconduct; and

(4) The person with operational responsibility for the ethics and compliance program has "direct reporting obligations" to the board of directors or an appropriate committee of the board, such as the Audit Committee.

Once again, the simplicity of these changes masks their wide-ranging significance. The first requirement places new weight on the initial reporting, review and investigation of any serious compliance matter. Are there processes in place—whether through internal audits, whistleblower hotlines, compliance reviews or other sources—for the company to find out first if something may be going wrong in the organization and to respond aggressively and intelligently to these reports?

The second requirement raises questions about what it means to report "promptly"; it places more pressure on the already difficult decision of whether and when to self-report possible violations to the authorities.

The last requirement energized the debate about whether an organization's chief compliance officer should report to the CEO or the board, rather than to a subordinate officer such as the general counsel. An Application Note accompanying this change provides that the individual in question should have explicit authority to report to the board about matters involving possible criminal wrongdoing and should report at least annually on the implementation and effectiveness of the compliance program. However, these changes to the guidelines do not necessarily, for all companies, require that the chief compliance officer report to the CEO or the board in a direct supervisory sense. Regardless of where the chief compliance officer stands in the organizational hierarchy, the organization should formalize his or her duty to report periodically to the board or a committee of the board about the state of the compliance program and any significant issues or problems. A board resolution is one good way to accomplish this.

We will consider all three issues in greater detail later in the chapter.

The Sentencing Commission also issued guidance regarding one of the elements of an "effective" compliance program—the appropriateness of the organization's response to criminal conduct. A recent application note directs organizations to take reasonable steps to remedy any harm resulting from the wrongdoing, such as by providing restitution, and reinforces the importance of self-reporting and cooperation with the authorities.

The current version of the FSGO can be found in Appendix 13-A to this chapter.

[vi] *Impact of the FSGO*

The Sentencing Commission has succeeded, perhaps beyond even its own expectations, in promoting the growth of organizational compliance programs and the adoption of codes of conduct as part of these programs. Its "elements of an effective compliance program" have become—as we shall see in subsequent sections of this chapter—common elements of compliance programs regardless of the industry and irrespective of whether the organization using them has ever been investigated or prosecuted for a federal crime.

Companies have developed compliance programs based on these elements in response to industry regulations, in an effort to adopt "best practices" or simply for protection in the event of federal prosecution if any employees do engage in misconduct. Because of the institutional and regulatory benefits of implementing the Guidelines, and the risks and consequences of inaction, it is prudent for a company to adopt a compliance program incorporating these standards. According to the report of the Ad Hoc Advisory Group, "there is abundant evidence that the organizational sentencing guidelines have, directly and indirectly, galvanized organizations to focus on their responsibility to detect and prevent violations of law and to institute compliance programs toward this goal."[38]

This influence far exceeds the direct impact of the FSGO in the federal courts. According to a report by the Conference Board, from 1993 through 2008, only three of the 2,811 sentenced organizations received any credit for having an effective compliance program.[39] In its 2018 Annual Report and Sourcebook of Federal Sentencing Statistics, the Sentencing Commission noted that, of the 54 of 99 cases for which they had sufficient information regarding the application of fine guidelines, only one of the 54 organizations sentenced that year saw its culpability score reduced for having an "effective" compliance program, although 49 organizations did get credit for self-reporting, cooperating with the authorities and/or accepting responsibility, which can still result in a percentage reduction off of the guidelines fine range. Similar results were reported in prior years.[40] Anticipating results like these, the Ad Hoc Advisory Group noted that:

> The extremely small number . . . is potentially misleading because it seriously understates the value of an effective compliance program. A number of government programs offer leniency to organizations that self-report violations in a timely manner, such as the U.S. Department of Justice's Antitrust Division's Corporate Amnesty policy. Moreover, the key regulatory and enforcement agencies, including the SEC and

---

[38] Ad Hoc Advisory Group Report at 29.

[39] Ethics and Compliance Enforcement Decisions: The Information Gap, The Conference Board, June 2009, *available at* www.conference-board.org.

[40] U.S. Sentencing Commission, Annual Report and Sourcebook 2018, at Table O-4, *available at* https://www.ussc.gov/sites/default/files/pdf/research-and-publications/annual-reports-and-sourcebooks/2018/TableO4.pdf.

> the Department of Justice, continue to use the elements of the FSGO as *their* guide in determining how organizations should be treated. Current and former U.S. Justice Department officials have stated to the Advisory Group that the Department has declined prosecutions based on the existence of an effective compliance program. An effective compliance program enables organizations to detect violations at an earlier stage than might otherwise occur, and it may thus give them the opportunity to self-report and qualify for lenient treatment under government policies.[41]

In announcing a deferred prosecution agreement with Johnson & Johnson ("J&J") to settle Foreign Corrupt Practices Act ("FCPA") violations in 2011, the DOJ noted that it agreed to this settlement, including a fine that was 25% below the bottom of the FSGO range, because J&J"has a pre-existing compliance and ethics program that was effective," voluntarily disclosed the misconduct following a thorough internal investigation, cooperated fully and had initiated "extensive remedial efforts."[42] Similarly, as part of its recent FCPA Pilot Program (discussed more fully below), the DOJ took the rare move of declining to press any charges against Nortek, Inc., a residential and commercial building products manufacturer, "despite the bribery by employees of the Company's subsidiary in China," in part because "Nortek's internal audit function identified the misconduct."[43] However, as the DOJ and SEC have reiterated, merely having a compliance program is not enough—it must be *effective*. For example, in 2015, BHP Billiton paid $25 million to settle FCPA charges by the SEC relating to BHP's hosting of foreign officials at the Beijing Summer Olympics. In announcing the settlement, Antonia Chion, Associate Director of the SEC's Division of Enforcement, explained that "[a]lthough BHP Billiton put some internal controls in place around its Olympic hospitality program, the company failed to provide adequate training to its employees and did not implement procedures to ensure meaningful preparation, review, and approval of the invitations," concluding that "[a] 'check the box' compliance approach of forms over substance is not enough to comply with the FCPA."[44]

[b] The Holder Memorandum

In 1999, the DOJ officially added its voice to the guidance received by organizations regarding compliance programs, by issuing for all federal prosecutors a document entitled *Bringing Criminal Charges Against Corporations*.[45] The "Holder Memorandum," named after then-Deputy Attorney General (later Attorney General) Eric Holder,

---

[41] Ad Hoc Advisory Group Report at 26–27.

[42] "Johnson & Johnson Agrees to Pay $21.4 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act and Oil for Food Investigations" (April 8, 2011), *available at* http://www.justice.gov/opa/pr/2011/April/11-crm-446.html.

[43] "Nortek, Inc. Declination Letter" (June 3, 2016), *available at* https://www.justice.gov/criminal-fraud/file/865406/download.

[44] "SEC Charges BHP Billiton With Violating FCPA at Olympic Games" (May 20, 2015), *available at* https://www.sec.gov/news/pressrelease/2015-93.html.

[45] *See* Office of the Deputy Attorney General, Bringing Criminal Charges Against Corporations (attaching the document "Federal Prosecution of Business Organizations") (June 16, 1999) [hereinafter Holder Memorandum], *available at* https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2010/04/11/charging-corps.PDF.

provided "guidance as to what factors should generally inform a prosecutor in making the decision whether to charge a corporation in a particular case." By its terms, this document moved questions about what constitutes an acceptable compliance program from the end of the criminal justice process—the sentencing of convicted organizations—to more frequent, and earlier, pre-charging decision-making by prosecutors.

The Holder Memorandum devoted a section to corporate compliance programs. This section began by noting that the DOJ "encourages such corporate self-policing, including voluntary disclosures to the government of any violations that a corporation discovers on its own."[46] The Memorandum then followed with the warning that "the existence of a compliance program is not sufficient, in and of itself, to justify not charging a corporation for criminal conduct undertaken by its officers, directors, employees, or agents. Indeed, the commission of such crimes in the face of a compliance program may suggest that corporate management is not adequately enforcing its program."

Nonetheless, a compliance program could make a difference, according to the Holder Memorandum, especially with regard to whether the corporation would be criminally charged for the misdeeds of its employees:

> Prosecutors should . . . attempt to determine whether a corporation's compliance program is merely a "paper program" or whether it was designed and implemented in an effective manner . . . In addition, prosecutors should determine whether the corporation's employees are adequately informed about the compliance program and are convinced of the corporation's commitment to it. This will enable the prosecutor to make an informed decision as to whether the corporation has adopted and implemented a truly effective compliance program that, when consistent with other federal law enforcement policies, may result in a decision to charge only the organization's employees and agents.[47]

The memorandum explained that the DOJ did not have its own "formal guidelines for effective compliance programs," and it specifically referred prosecutors to the FSGO "[f]or a detailed review of these and other factors concerning corporate compliance programs."[48]

[c] The Thompson Memorandum

Three and a half years after issuing the Holder Memorandum, in the midst of the Enron investigation and other corporate scandals, the DOJ revised its guidance for prosecutors who were deciding whether to charge organizations with federal crimes. On January 20, 2003, the Department issued the "Thompson Memorandum," named for its author, then-Deputy Attorney General Larry D. Thompson, who was also head of the President's Corporate Fraud Task Force. This document, entitled *Principles of Federal*

---

[46] Holder Memorandum at § VII(A).

[47] Holder Memorandum at § VII(B).

[48] Holder Memorandum at § VII(B).

Prosecution of Business Organizations, reaffirmed the guidance in the Holder Memorandum, with some variation.[49]

The section devoted to compliance programs provided that federal prosecutors, in "conducting an investigation, determining whether to bring charges, and negotiating plea agreements" should consider, among a number of factors, "the existence and adequacy of the corporation's compliance program."[50] This section largely repeated the corresponding section of the Holder Memorandum, including the references to the FSGO and related compliance guidance from various regulators. Prosecutors had to ask the same questions that corporate counsel should be asking about the organization's compliance program: "Is the compliance program well-designed?" and "Does the corporation's compliance program work?" Among the issues that prosecutors should review are whether the organization's compliance program is "designed to detect the particular types of misconduct most likely to occur" in its line of business and whether the program has been given "staff sufficient to audit, document, analyze, and utilize the results" of its compliance efforts.

Federal prosecutors were urged to determine whether the organization had established "corporate governance mechanisms" to prevent and detect misconduct:

> [A]re the directors provided with information sufficient to enable the exercise of independent judgment; are internal audit functions conducted at a level sufficient to ensure their independence and accuracy and have the directors established an information and reporting system in the organization reasonably designed to provide management and the board of directors with timely and accurate information sufficient to allow them to reach an informed decision regarding the organization's compliance with the law.[51]

The Thompson Memorandum also echoed the recommendation of its predecessor that a prosecutor should consider a corporation's remedial actions once misconduct has been revealed, "including any efforts to implement an effective corporate compliance program or to improve an existing one, to replace responsible management, to discipline or terminate wrongdoers, to pay restitution, and to cooperate with the relevant government agencies."[52]

One change in the Thompson Memorandum proved especially contentious. It instructed prosecutors to increase their "emphasis on and scrutiny of the authenticity of a corporation's cooperation" with the government. In deciding whether to charge an organization, prosecutors were to consider the organization's "timely and voluntary disclosure of wrongdoing and its willingness to cooperate in the investigation of its

---

[49] Office of the Deputy Attorney General, Principles of Federal Prosecution of Business Organizations (attaching revisions to the Holder Memorandum) (Jan. 20, 2003) [hereinafter Thompson Memorandum], *available at* https://www.americanbar.org/content/dam/aba/migrated/poladv/priorities/privilegewaiver/2003jan20_privwaiv_dojthomp.authcheckdam.pdf and reproduced in its current form in Appendix 13-B to this chapter.

[50] Thompson Memorandum at § VII (Charging a Corporation: Corporate Compliance Programs).

[51] Thompson Memorandum at § VII (Charging a Corporation: Corporate Compliance Programs).

[52] Thompson Memorandum at § VIII (Charging a Corporation: Restitution and Remediation).

agents, including, if necessary, the waiver of corporate attorney-client privilege and work product protection." The Memorandum further explained that, in assessing an organization's cooperation, prosecutors should determine if the company has retained errant employees without sanction or advanced attorneys' fees to employees under investigation. Among the difficult issues that the memorandum raised was whether the government would expect or require that an organization waive its attorney-client protections to receive credit for cooperation.[53]

A coalition of corporate counsel, defense attorneys and business groups including the Business Roundtable and the U.S. Chamber of Commerce was organized to resist this perceived effort to weaken the attorney-client privilege. One outcome of the efforts of this Coalition to Preserve Attorney-Client Privilege was the introduction in the 110th Congress by then-Senator Arlen Specter (R-Pa) of the "Attorney-Client Privilege Act of 2007." The Act stated that "the ability of an organization to have effective compliance programs and to conduct comprehensive internal investigations is enhanced when there is clarity and consistency regarding the attorney-client privilege." As such, the proposal generally prohibited federal prosecutors from demanding waiver of the privilege from an organization under investigation or from conditioning "a civil or criminal charging decision" on "any valid assertion of the attorney-client privilege or privilege for attorney work product."[54] On February 13, 2009, the Act was reintroduced by Senator Specter but was not acted on by Congress.[55]

In the meantime, application of the Thompson Memorandum was successfully challenged in a prosecution of former KPMG employees, in which a federal district court issued three successive rulings.[56] In the first ruling, the court found that pressure from prosecutors, based on the Thompson Memorandum, caused KPMG to refuse to advance attorneys' fees for its current and former employees, reversing longstanding company policy. Such pressure, the court held, violated the individual defendants' Fifth and Sixth Amendment rights. In the second ruling, the court suppressed statements made by two of the defendants following threats by KPMG to fire them if they did not cooperate with the government. In the court's view, "the government is responsible for the pressure that KPMG put on its employees. It threatened KPMG with the corporate equivalent of capital punishment. KPMG took the only course open to it."[57]

In the third ruling, dismissing the charges against 13 of the individual defendants, the court concluded that the prosecution's application of the Thompson memorandum violated due process because none of the defendants had "the resources to defend this

---

[53] Thompson Memorandum at § VI (Charging a Corporation: Cooperation and Voluntary Disclosure).

[54] Attorney-Client Privilege Protection Act of 2007, S.186, 110th Cong. (2007), *available at* https://www.congress.gov/bill/110th-congress/senate-bill/186/text.

[55] Attorney-Client Privilege Protection Act of 2009, S. 445, 111th Cong. (2009), *available at* https://www.congress.gov/bill/111th-congress/senate-bill/445/text.

[56] *See* U.S. v. Stein, 435 F. Supp. 2d 330 (S.D.N.Y. 2006); U.S. v. Stein, 440 F. Supp. 2d 315 (S.D.N.Y. 2006); U.S. v. Stein, 495 F. Supp. 2d 390 (S.D.N.Y. 2007). *See also* Stein v. KPMG, LLP, 486 F.3d 753 (2d Cir. 2007).

[57] U.S. v. Stein, 440 F. Supp. 2d 315, 319 (S.D.N.Y. 2006).

case as he or she would have" had the prosecutors not "prevented" KPMG from continuing to pay their defense costs. The government's "deliberate interference with the defendants' rights was outrageous and shocking in the constitutional sense because it was fundamentally at odds with two basic constitutional values—the right to counsel and the right to fair criminal proceedings."[58]

These opinions led the Justice Department to issue yet another memorandum on this subject.

[d] The McNulty Memorandum

On December 12, 2006, then-Deputy Attorney General Paul McNulty issued a memorandum superseding the Thompson Memorandum.[59] While the McNulty Memorandum carried over many of the principles of the Holder and Thompson Memoranda, it departed from the prior guidance in two significant ways. The changes largely reflected the pressure from defense lawyers, bar associations and others—as well as litigation, court decisions and the proposed legislation—in response to the Department of Justice's policies and practices in the areas of (a) waivers of the attorney-client privilege and (b) corporations' advancement of legal fees to subjects and targets of investigations.

The McNulty Memorandum required that federal prosecutors seek written approval within the Department of Justice before requesting waivers of the attorney-client privilege or work product protection. In remarks accompanying release of his memorandum, Deputy Attorney General McNulty asserted that "attorney-client communications should only be sought in rare cases." The Memorandum then detailed the test that prosecutors must meet in order to demonstrate these uncommon circumstances. Further, the McNulty Memorandum generally prohibited prosecutors, in assessing companies' cooperation with the government, from considering whether these companies were advancing attorneys' fees to their employees or agents. In announcing these concessions, Deputy Attorney General McNulty challenged corporations to "prevent corruption through self-policing and continue to punish wrongdoers through cooperation with law enforcement."

Contrary to the Justice Department's hope, the McNulty memorandum did not end the debate or the pressure to modify its approach to corporate cooperation and privilege.

[e] The Filip Letter and Memorandum

On July 28, 2008, then-Deputy Attorney General Mark Filip sent a letter to Senators Patrick Leahy and Arlen Specter informing them that he had completed an internal review of the Justice Department's Principles of Federal Prosecution of Business Organizations. He did so in response to the continuing claim that the Department was forcing corporations to waive their attorney-client and work product privileges in order to get credit under these principles for cooperating with the government. He also was

---

[58] U.S. v. Stein, 495 F. Supp. 2d 390, 414 (S.D.N.Y 2007).

[59] P. McNulty, Principles of Federal Prosecution of Business Organizations, *available at* http://www.usdoj.gov/dag/speeches/2006/mcnulty_memo.pdf.

responding to concerns, reflected in the KPMG case, that the Department was improperly limiting or refusing to grant cooperation credit when "the corporation has advanced attorneys' fees to its employees, failed to fire or sanction allegedly culpable employees, or entered into joint defense agreements."

In August 2008, following a series of meetings the Department held with in-house counsel, criminal defense attorneys and other interested parties, the Justice Department completed revisions to the Principles to address these issues. These revisions provide that:

- Cooperation by organizations will be determined based on the facts that are disclosed to the prosecution, not by the waiver of privileges.
- Prosecutors will not insist on the disclosure of "core attorney-client privileged communications" or "non-factual" work product before granting cooperation credit.
- Prosecutors will not consider either the advancement of attorneys' fees or joint defense agreements in evaluating cooperation.
- In evaluating the organization's compliance program, but not in assessing its cooperation, the government will consider whether and how a company disciplines its employees.[60]

Most important for purposes of this chapter, this revised version of the Principles maintains the emphasis on whether the corporation being sentenced has an effective compliance program, reiterating the language from the Holder Memorandum that a corporation's adoption of "a truly effective compliance program . . . may result in a decision to charge only the corporation's employees and agents or to mitigate charges or sanctions again the corporation." This emphasis in the revised Principles substantiates one of the underlying principles of this chapter: A compliance program can prevent violations of law or regulations or, in the case of violations by individual employees, can help insulate a company from prosecution or an enforcement action.

The current version of the Principles of Federal Prosecution of Business Organizations can be found in Appendix 13-B to this chapter.

[f] The FCPA Guide

On November 14, 2012, the Criminal Division of the DOJ and the Enforcement Division of the SEC jointly issued A Resource Guide to the FCPA. This long-awaited and eagerly-anticipated resource "endeavors to provide helpful information to enter-

---

[60] The SEC's Division of Enforcement has adopted similar language in guidance for its staff: "A party's decision to assert a legitimate claim of attorney-client privilege or work product protection will not negatively affect their claim to credit for cooperation. The appropriate inquiry in this regard is whether, notwithstanding a legitimate claim of attorney-client privilege or work product protection, the party has disclosed all relevant underlying facts within its knowledge." U.S. Securities and Exchange Commission, Division of Enforcement, Enforcement Manual, Nov. 28, 2017 at 77. Any requests to parties for a waiver of these protections require prior approval of the Director or Deputy Director of the Division.

prises of all shapes and sizes . . . . The Guide is an unprecedented undertaking by DOJ and SEC to provide the public with detailed information about our FCPA approach and priorities."[61]

While oriented towards FCPA investigations and prosecutions, the Guide has a section on the Hallmarks of Effective Compliance Programs, which includes the following subsection about Codes of Conduct and Compliance Policies and Procedures:

> A company's code of conduct is often the foundation upon which an effective compliance program is built. As DOJ has repeatedly noted in its charging documents, the most effective codes are clear, concise and accessible to all employees and to those conducting business on the company's behalf . . . . When assessing a compliance program, DOJ and SEC will review whether the company has taken steps to make certain that the code of conduct remains current and effective and whether a company has periodically reviewed and updated its code. *See Id.* at 57–58.

The Guide goes on to offer concrete evidence that "DOJ and SEC will give meaningful credit to thoughtful efforts to create a sustainable compliance program [even] if a problem is later discovered."[62] The Guide offers six examples of cases in which the government declined to prosecute.[63] In these cases, the company's own compliance program and internal controls discovered the problem, which the company then voluntarily disclosed to the SEC and/or DOJ.

This Guide is an unprecedented, joint expression by the DOJ and SEC of the practical value—and expected elements of—organizational compliance programs. As such, its importance extends beyond the FCPA.

[g] The Yates Memorandum

On September 9, 2015, then-Deputy Attorney General Sally Yates circulated a memo to all DOJ prosecutors, entitled "Individual Accountability for Corporate Wrongdoing."[64] The purpose of the memo was to outline the Department's new focus on "combat[ing] corporate misconduct . . . by seeking accountability from the individuals who perpetrated the wrongdoing"; that is, seeking to punish—including with "incarceration, fines, penalties, damages, restitution to victims, asset seizure, civil and criminal forfeiture, and exclusion, suspension and debarment"—the culpable individuals who led and participated in the corporate wrongdoing, rather than just punishing the corporate entity with fines and other sanctions. Deputy AG Yates thus instructed U.S. Attorneys to "fully leverage [the DOJ's] resources to identify culpable individuals at all levels in corporate cases," and delineated "six key steps" (some of which she described as "policy shifts") aimed at accomplishing this goal of "strengthen[ing] our pursuit of individual corporate wrongdoing":

---

[61] *See* the Foreword to the Guide, which is available at https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf.

[62] *Id.* at 62.

[63] *See id.* at 77–79.

[64] Sally Quillian Yates, Individual Accountability for Corporate Wrongdoing (Sep. 9, 2015), *available at* https://www.justice.gov/dag/file/769036/download.

1. To qualify for "*any*" cooperation credit, corporations must completely disclose "all relevant facts relating to the individuals responsible for the misconduct," regardless of the individual's position in the company or seniority;
2. Prosecutors "should focus on individuals from the inception of the investigation";
3. Criminal and civil prosecutors "should be in routine communication with one another";
4. DOJ "will not release culpable individuals from civil or criminal liability when resolving a matter with a corporation," except in "extraordinary circumstances or [pursuant to] approved departmental policy";
5. Prosecutors should not resolve corporate investigations "without a clear plan to resolve related individual cases"; and
6. Civil prosecutors should "evaluate whether to bring suit against an individual based on considerations beyond that individual's ability to pay."[65]

Of the six "steps," the first one—setting out the new standard for cooperation credit—is the most important from the perspective of corporate compliance. As Deputy AG Yates noted in her speech introducing these changes, this new approach marks a "substantial shift from [the DOJ's] prior practice" as outlined in the Filip memo, in that the Department will no longer award "partial credit for cooperation that doesn't include information about individuals."[66] Crucially, companies will not be permitted to "plead ignorance" of individual culpability: "If they don't know who is responsible, they will need to find out. If they want any cooperation credit, they will need to investigate and identify the responsible parties, then provide all non-privileged evidence implicating those individuals."[67] This new standard, then, makes having an effective and robust compliance program—with mechanisms for reporting and investigation misconduct—more important than ever. Companies without compliance programs and reporting structures to keep them apprised of individual wrongdoing will be either unable to receive cooperation credit, or else will have to expend a significant amount of money to bring in outside resources to help them uncover the necessary information.

---

[65] *Id.* (emphasis added).

[66] Sally Quillian Yates, Remarks at New York University School of Law Announcing New Policy on Individual Liability in Matters of Corporate Wrongdoing (Sept. 10, 2015), *available at* https://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school. The principles outlined in Deputy AG Yates's memo and related speeches have been incorporated, with some modification, into the current version of the Principles of Federal Prosecution of Business Organizations, found in Appendix 13-B to this chapter.

[67] *Id.*

[h] FCPA Corporate Enforcement Policy

On November 29, 2017, then-Deputy Attorney General Rod Rosenstein announced a revised FCPA Corporate Enforcement Policy based upon the results of the FCPA Pilot Program.[68]

The FCPA Pilot Program had been instituted in April 2016 and was meant to incentivize companies to voluntarily self-disclose FCPA-related misconduct and to more actively cooperate with DOJ investigations. A review of the Pilot Program found that "during the year and a half that the Pilot Program was in effect, the FCPA Unit received 30 voluntary disclosures compared to 18 during the previous 18-month period."[69] Deputy AG Rosenstein touted these figures when he announced the revised Corporate Enforcement Policy. While the new policy creates no private rights and is not enforceable in court, it was intended to promote consistency by attorneys throughout the DOJ by guiding the exercise of discretion to prevent arbitrary outcomes. Its goal is to provide businesses with more transparency about the costs and benefits of cooperation, and therefore specifies what is meant by voluntary disclosure, full cooperation, and timely and appropriate remediation.[70] The new policy, similar to the FCPA Pilot Program, continues to require that companies pay disgorgement of ill-gotten gains, forfeiture and restitution to qualify for leniency.

Under the FCPA Corporate Enforcement Policy, companies that: (1) voluntarily self-disclose, (2) cooperate fully with the investigation (including, per the Yates Memo and Rosenstein's subsequent comments, by disclosing all facts related to involvement by individuals) and (3) timely and appropriately remediate the misconduct will be afforded a rebuttable presumption that their case will be resolved with a declination of prosecution. This presumption may be overcome in cases with aggravating circumstances involving the seriousness of the offense or the nature of the offender. In such cases, a company will receive, or the DOJ will recommend to a sentencing court, a 50% reduction off the bottom of the applicable Sentencing Guidelines fine range (unless the company is determined to be a criminal recidivist). Furthermore, the DOJ "generally will not require appointment of a monitor if a company has, at the time of resolution, implemented an effective compliance program."[71] Companies that cooperate and remediate but do not self-disclose may receive the benefit of an up to 25% reduction off the bottom of the applicable Sentencing Guidelines fine range.[72]

Similar to the pilot program, the FCPA Corporate Enforcement Policy requires the implementation of an effective compliance and ethics program in order to receive full

---

[68] Remarks as prepared for delivery by Rod Rosenstein, "Deputy Attorney General Rosenstein Remarks at the 34th International Conference on the Foreign Corrupt Practices Act" (Nov. 29, 2017), *available at* https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-34th-international-conference-foreign.

[69] *Id.*

[70] *Id.*

[71] USAM Insert 9-47.120—FCPA Corporate Enforcement Policy (November 29, 2017). *See* Section 13.02[3][a], *infra*, for further discussion of the government's use of independent compliance monitors.

[72] *Id.*

credit for timely and appropriate remediation. The factors considered under the Corporate Enforcement Policy are generally the same as those that were considered under the predecessor pilot program, including:

1. "The company's culture of compliance, including awareness among employees that any criminal conduct, including the conduct underlying the investigation, will not be tolerated;
2. The resources the company has dedicated to compliance;
3. The quality and experience of the personnel involved in compliance, such that they can understand and identify the transactions and activities that pose a potential risk;
4. The authority and independence of the compliance function and the availability of compliance expertise to the board;
5. The effectiveness of the company's risk assessment and the manner in which the company's compliance program has been tailored based on that risk assessment;
6. The compensation and promotion of the personnel involved in compliance, in view of their role, responsibilities, performance, and other appropriate factors;
7. The auditing of the compliance program to assure its effectiveness; and
8. The reporting structure of any compliance personnel employed or contracted by the company."[73]

However, unlike the pilot program, the FCPA Corporate Enforcement Policy makes clear that the criteria "will be periodically updated and [] may vary based on the size and resources of the organization."[74] The DOJ has also announced several expansions to the scope of the Corporate Enforcement Policy:

In March 2018, then-Acting Attorney General John Cronan announced that the Criminal Division would begin considering the FCPA Corporate Enforcement Policy as "nonbinding guidance" in all corporate criminal cases, not just those involving the FCPA.[75]

On July 25, 2018, the DOJ announced that the Corporate Enforcement Policy also applies to mergers and acquisitions that uncover potential FCPA violations.[76] Namely, successor companies that identify potential FCPA violations in connection with a

---

[73] *Id.*

[74] *Id.*

[75] *See* Remarks as prepared for delivery by Mathew S. Miner, "Deputy Assistant Attorney General Matthew S. Miner of the Justice Department's Criminal Division Delivers Remarks at the 5th Annual GIR New York Live Event" (Sept. 27, 2018), *available at* https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matthew-s-miner-justice-department-s-criminal-division.

[76] Remarks as prepared for delivery by Matthew S. Miner, "Deputy Attorney General Matthew S. Miner Remarks at the American Conference Institute 9th Global Forum on Anti-Corruption Compliance in High Risk Markets" (July 25, 2018), *available at* https://www.justice.gov/opa/pr/deputy-assistant-attorney-general-matthew-s-miner-remarks-american-conference-institute-9thn.

merger and disclose the conduct to the DOJ will be treated in conformance with the policy. On September 27, 2018, the DOJ also announced that the same principles will apply to mergers that uncover other types of potential wrongdoing, not just FCPA violations.[77]

On March 8, 2019, the DOJ announced an update to the Corporate Enforcement Policy requiring "appropriate retention of business records." Previously, to demonstrate "appropriate retention of business records," companies had to have a policy in place that prevented employees from using software that did not appropriately retain business records, including WhatsApp, Snapchat, and other messaging applications.[78] Under the new update, the blanket prohibition was removed, and companies instead must implement "appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications."[79] The amended policy, however, does not elaborate or provide guidance on what constitutes "appropriate guidance and controls."

In the first quarter of 2019, the DOJ announced three corporate FCPA enforcement actions against Cognizant Technology Solutions Corporation, Fresenius Medical Care AG & Co. KGaA, and Mobile TeleSystems Public Joint Stock Company ("MTS"), representing a declination, a non-prosecution agreement and a deferred prosecution agreement, respectively. The resolution with MTS was one of the biggest resolutions of all time, and in total, the three companies paid just over $1.1 billion.

The three resolutions demonstrate the significance of voluntary disclosure, full cooperation, and timely and appropriate remediation under the Policy. In announcing the declination with Cognizant, the DOJ explained that "[c]onsistent with the Corporate Enforcement Policy," the Department declined to charge the company based upon "(1) Cognizant's voluntary self-disclosure . . . within two weeks of the Board learning of the criminal conduct; (2) Cognizant's thorough and comprehensive investigations; [and] (3) Cognizant's full and proactive cooperation in this matter."[80] In the case of Fresenius, the Company did receive voluntary disclosure credit and partial credit for cooperation, but was not entitled to a declination because "it did not timely respond to request by the Department and, at times, did not provide fulsome responses to requests for information."[81] Finally, with respect to MTS, the DOJ noted a number of factors

---

[77] Remarks as prepared for delivery by Mathew S. Miner, "Deputy Assistant Attorney General Matthew S. Miner of the Justice Department's Criminal Division Delivers Remarks at the 5th Annual GIR New York Live Event" (Sept. 27, 2018), *available at* https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matthew-s-miner-justice-department-s-criminal-division.

[78] USAM Insert 9-47.120—FCPA Corporate Enforcement Policy (November 29, 2017).

[79] USAM Insert 9-47.120—FCPA Corporate Enforcement Policy (March 8, 2019).

[80] Letter from Craig Carpenito, U.S. Attorney, Dist. of N.J., et al., to Karl H. Buch, Counsel for Cognizant, and Kathryn H. Ruemmler, Counsel for Cognizant (Feb. 3, 2019), *available at* https://www.justice.gov/criminal-fraud/file/1132666/download.

[81] Letter from Robert Zink, Acting Chief, Fraud Section, Criminal Div., U.S. Dept. of Justice, et al.,

that contributed to the decision to pursue a deferred prosecution agreement, including that "the company[y] did not voluntary disclose [and] the . . . level of cooperation and remediation was lacking, not proactive."[82]

Through the Corporate Enforcement Policy, the DOJ has highlighted the importance of both having an effective compliance program that can proactively identify and correct wrongdoing, and also instilling a "culture of compliance" throughout the organization. When companies can demonstrate that they have a robust compliance program and that they take compliance seriously, they make themselves eligible for either no—or at least significantly reduced—penalties.

[i] "Evaluation of Corporate Compliance Programs"

More recently, in April 2019, the Fraud Section of the DOJ's Criminal Division updated a DOJ guidance document entitled "Evaluation of Corporate Compliance Programs" ("Evaluation Memorandum"), which was originally published in February 2017. The Evaluation Memorandum "is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution,"[83] by "providing additional context to the multifactor analysis of a company's compliance program."[84] It contains important topics and sample questions that the Fraud Section has frequently found relevant in evaluating a corporate compliance program for purposes of the Filip Memorandum.[85] These topics—similar to those already appearing in the FSGO and the FCPA Guide—"form neither a checklist nor a formula," with each being more or less relevant depending on the particular facts of the criminal investigation at issue.[86] The guidance document is divided into three main categories, presented as questions, measured by twelve criteria:

1. "**Is the Corporation's Compliance Program Well Designed?**"

This section evaluates whether a company's compliance program is designed to effectively prevent and detect wrongdoing by employees, and what role the company's

---

to Maxwell Carr-Howard, Counsel for Fresenius (Feb. 25, 2019), *available at* https://www.justice.gov/criminal-fraud/file/1150566/download.

[82] Press Release, U.S. Dep't of Justice, Mobile Telesystems Pjsc and Its Uzbek Subsidiary Enter into Resolutions of $850 Million with the Department of Justice for Paying Bribes in Uzbekistan: Former General Director of MTS's Uzbek Subsidiary and Former Uzbek Official Charged in Bribery and Money Laundering Scheme Totaling Almost $1 Billion (March 7, 2019), *available at* https://www.justice.gov/opa/pr/mobile-telesystems-pjsc-and-its-uzbek-subsidiary-enter-resolutions-850-million-department.

[83] U.S. Dep't of Just., Criminal Division, Fraud Section, Evaluation of Corporate Compliance Programs (April 30, 2019), *available at* https://www.justice.gov/criminal-fraud/page/file/937501/download.

[84] Press Release, U.S. Dep't of Justice, Criminal Division Announces Publication of Guidance on Evaluating Corporate Compliance Programs (April 30, 2019), *available at* https://www.justice.gov/opa/pr/criminal-division-announces-publication-guidance-evaluating-corporate-compliance-programs.

[85] U.S. Dep't of Just., Criminal Division, Fraud Section, Evaluation of Corporate Compliance Programs (Feb. 8, 2017), *available at* https://www.justice.gov/criminal-fraud/page/file/937501/download.

[86] *Id.*

management plays in promoting, or deterring, compliance. There are six measures in this section:

- "Risk Assessment," including what methodology the company has used to identify, analyze and address the particular risks it faces, and the quality and effectiveness thereof.
- "Policies and Procedures," including whether the company has an accessible code of conduct that sets forth the company's commitment to full compliance with relevant Federal law; and whether the company's policies and procedures incorporate a culture of compliance into everyday operations.
- "Training and Communications," including whether the company adequately and periodically trains employees about its compliance program and provides easily accessible guidance related to its compliance policies.
- "Confidential Reporting Structure and Investigation Process," including the existence of an anonymous/confidential mechanism for employees to report breaches of the company's code of conduct, and effective procedures for responding.
- "Third Party Management," including how the company's third-party management process takes account of the level of risk of the particular third party at issue and how the company monitors third parties and promotes their compliance and ethical behavior.
- "Mergers and Acquisitions," including whether the company's compliance program includes comprehensive due diligence of any acquisition targets and processes for implementing proper compliance policies at new entities.

2. "**Is the Corporation's Compliance Program Being Implemented Effectively?**"

This section evaluates how well the compliance program is implemented in practice, as it is insufficient to merely design a compliance program without creating a culture of compliance at all levels. There are three measures in this section:

- "Commitment by Senior and Middle Management," including the conduct, commitment and oversight of senior and middle management in fostering and displaying a culture of ethics and compliance with the law.
- "Autonomy and Resources," including how the compliance function compares with other strategic functions in the company in terms of stature, compensation, title, resources and access to key decision-makers; whether the compliance and other relevant control functions are "conducted at a level to ensure their independence and accuracy";[87] and how the company has responded to instances, if any, where the compliance function raised concerns or objections.
- "Incentives and Disciplinary Measures," including how the company has positively incentivized compliance and ethical behavior; how the company has communicated that unethical conduct and non-compliance will not be tolerated,

[87] *Id.* at 11.

regardless of the employee's title or position; and whether disciplinary actions are in fact enforced consistently across the entity.

3. "**Does the Corporation's Compliance Work in Practice?**"

This section evaluates how well a company's compliance program worked at the time of alleged misconduct in comparison to the time of prosecution. After all, no compliance program will prevent or detect every act of misconduct, so the guidance reflects an expectation that companies constantly assess and improve their compliance programs, particularly after lapses are identified. There are three measures in this section:

- "Continuous Improvement, Periodic Testing, and Review," including whether and how often the company reviews and audits its compliance program; how results of such reviews are reported and tracked; how often the company updates its risk assessment and reviews its compliance policies and practices; and whether and how often the company measures its culture of compliance, including whether the company seeks inputs from employees on all levels and what steps the company takes in response to that input.
- "Investigation of Misconduct," including whether the company's investigations are conducted by qualified personnel; the company's response to findings; and whether there are effective, established means of documenting the company's response.
- "Analysis and Remediation of Any Underlying Misconduct," including whether the company is able to conduct "a thoughtful root cause analysis of misconduct;"[88] whether there were prior opportunities to identify the misconduct in question (e.g., through internal audits); and what remediation the company has undertaken to address the root causes of misconduct in the past.

Although the topics and questions in the Evaluation Memorandum are more specific than whether a company has a culture of compliance or the right code of conduct, these topics and questions are helpful indicators of how the DOJ views an effective compliance culture and program overall.

[j] Recent DOJ Deferred Prosecution and Non-Prosecution Agreements

Looking at deferred prosecution and non-prosecution agreements that companies have entered into with the DOJ offers additional insight into how the DOJ views compliance programs. In particular, these agreements tend both to reflect the attributes of a company's compliance program or remediation that the government is crediting (*i.e.*, for purposes of the FSGO and in agreeing to avoid immediate prosecution), as well as to prescribe improvements the company must implement to make its compliance program fully effective. Both the credited attributes and the mandated enhancements illustrate what the DOJ looks for in effective compliance programs.

Under a deferred prosecution agreement, the DOJ files charges against the organization but agrees to defer prosecution, often for several years. In return, the company

[88] *Id.* at 16.

admits the facts that establish wrongdoing, agrees to cooperate with the government, makes a substantial financial payment and carries out a series of tasks or "undertakings" during this period, sometimes including accepting an independent corporate monitor.[89] If the company complies with the terms of the agreement, the charges are dismissed. If not, the DOJ can prosecute, armed now with the company's admissions.

In a variation of this agreement—the non-prosecution agreement—the government refrains from filing charges at all, in return for the company's similar acceptance of responsibility and willingness to implement the undertakings. While the tasks in each agreement reflect the specific charges and issues in the case, the list of undertakings invariably includes implementing or strengthening corporate governance and compliance-related provisions.

For example, in June 2016, under the FPCA Pilot Program, the DOJ announced a non-prosecution agreement with Analogic Corp. and its subsidiary BK Medical, regarding BK Medical's funneling of improper payments to third parties and covering it up with fake invoices, causing Analogic to falsify its books and records.[90] In connection with the pilot program, the DOJ awarded Analogic full credit for self-disclosure and approvingly noted its "extensive remedial measures," but did not credit it fully for cooperation because "the Company did not disclose information that was known to the Company and Analogic about the identities of a number of the state-owned entity end-users of the Company's products," contrary to the requirements of the Yates memo.[91] The company therefore received only a 30—rather than 50—percent reduction off the bottom of the Sentencing Guidelines range. However, noting Analogic's commitment "to continue to enhance its compliance program and internal controls," as well as "the state of its compliance program," the DOJ elected not to require the company to adopt an independent compliance monitor (a requirement discussed in greater detail, *infra*).[92]

In January 2017, the DOJ entered into non-prosecution agreement with Las Vegas Sands Corp. ("LVSC"), a Nevada-based casino and resort company, in settlement of foreign bribery charges for which the company agreed to pay a $6.9 million penalty.[93] Despite former executives' "willful failure" to implement adequate internal accounting controls, the company received credit for its extensive remedial measures, including revamping and expanding its compliance and audit functions.[94] The changes instituted by LVSC in the wake of the foreign bribery allegations included establishing a new Board of Directors Compliance Committee; and updating the Code of Business

---

[89] *See* § 13.02[3][a].

[90] *In re* BK Medical ApS Non-Prosecution Agreement 8 (June 21, 2016), *available at* https://www.justice.gov/opa/file/868771/download.

[91] *Id.*

[92] *Id.*

[93] Non-Prosecution Agreement between the U.S. Dep't. of Justice Criminal Division and Las Vegas Sands Corp., Jan. 17, 2017.

[94] *Id.* at 1–2.

Conduct, Anti-Corruption Policy, and other relevant policy guidelines.[95] Further, LVSC enhanced its financial controls, screening of third parties and new hires, and electronic procurement and contract management systems.[96] LVSC also retained an independent compliance consultant.[97] In recognition of these remedial measures and enhancements to LVSC's compliance program, the company received a 25 percent reduction from the FSGO fine range, and avoided criminal charges.[98]

In May 2017, Banamex USA, and its parent company, Citigroup Inc., also avoided criminal prosecution by strengthening compliance efforts and entering into a non-prosecution agreement with the DOJ.[99] However, under the agreement, Banamex not only forfeited $97 million to settle the Bank Secrecy Act violations, but Citigroup also agreed to dissolve the subsidiary all together. Banamex admitted to "willfully failing to maintain an effective anti-money laundering (AML) compliance program with appropriate policies, procedures, and controls to guard against money laundering."[100] According to the DOJ, Banamex employed a "limited and manual" monitoring system on the tens of millions of remittance transactions it processed.[101] As early as 2004, Banamex understood the need to enhance its anti-money laundering efforts with more resources and compliance staffing, yet failed to make these necessary changes.[102] The DOJ credited Banamex and Citigroup Inc. for their "extensive remedial measures" including devoting significant resources to remediation of AML deficiencies, enhancing the Bank Secrecy Act compliance program and internal controls, investing in enhanced transaction monitoring technology, and significantly increasing compliance staffing.[103] This case serves as a harsh reminder of the consequences a company can face for failing to provide the necessary resources and attention to its compliance program.

More recently, in April 2018, Panasonic Avionics Corporation ("PAC") entered into a deferred-prosecution agreement with the DOJ, in which it agreed to pay a criminal penalty of $137.4 million for alleged violations of the FCPA books and records provisions. Although the DOJ found that PAC's remediation was "untimely in certain respects," the company did receive some credit for its remediation, including causing several senior executives who were either involved in or aware of the misconduct to

---

[95] *Id.*

[96] *Id.*

[97] *Id.* at 2.

[98] *Id.* at 2, 4.

[99] Non-Prosecution Agreement between the U.S. Dep't. of Justice Criminal Division and Banamex USA, May 18, 2017 [hereinafter Banamex USA NPA].

[100] Press Release, U.S. Dep't of Justice, Banamex USA Agrees to Forfeit $97 Million in Connection with Bank Secrecy Act Violations (May 22, 2017), *available at* https://www.justice.gov/opa/pr/banamex-usa-agrees-forfeit-97-million-connection-bank-secrecy-act-violations [hereinafter Banamex Press Release].

[101] Banamex USA NPA at Attachment A ¶ 3. From 2007–2012, Banamex processed more than 30 million remittance transactions to Mexico with a total value exceeding $8.8 billion. However, Banamex conducted fewer than 10 investigations. Banamex Press Release.

[102] Banamex USA NPA at Attachment A ¶ 5.

[103] *Id.* at 1.

separate from the company. The DOJ also noted that PAC had made enhancements to its compliance program; but because these enhancements "were more recent, and therefore ha[d] not been tested," the DOJ imposed an independent compliance monitor for a term of two years, followed by an additional year of self-reporting to the DOJ.[104] The DOJ reached a similar conclusion in March 2019 in Fresenius Medical Care, *supra*.[105] These cases suggest that to avoid the imposition of compliance monitors, companies should endeavor to make improvements to their compliance programs as early as possible after issues are identified.

Not all companies avoid criminal prosecution, either by way of declination or under deferred prosecution or non-prosecution agreements. In December 2016, Brazilian companies Odebrecht S.A. and Braskem S.A. each pleaded guilty to conspiring to violate the anti-bribery provisions of the FCPA and agreed to pay a combined $3.5 billion.[106] Odebrecht and Braskem used a hidden business unit, described by the DOJ as a "Department of Bribery," to funnel nearly one billion dollars in bribes to government officials and political parties on three continents.[107] The secret financial unit reported to the highest levels within the organization and used a complex network of shell companies, off-book transactions, and offshore bank accounts.[108]

Although the DOJ noted that Odebrecht lacked an effective compliance and ethics program at the time of the conduct, the government credited the company for its extensive remedial measures and full cooperation.[109] As a result, Odebrecht received a 25 percent reduction from the bottom of the applicable FSGO fine range.[110] The remedial measures undertaken by Odebrecht included: creating a chief compliance officer position that reports directly to the audit committee of the board of directors; adopting heightened controls and anti-corruption compliance protocols, including hospitality and gift approval procedures; incorporating adherence to compliance principles into employee performance evaluation and compensation; and increasing the number of employees and resources dedicated to compliance.[111] Odebrecht and

---

[104] Press Release, U.S. Dep't of Justice, Panasonic Avionics Corporation Agrees to Pay $137 Million to Resolve Foreign Corrupt Practices Act Charges (April 30, 2018), *available at* https://www.justice.gov/opa/pr/panasonic-avionics-corporation-agrees-pay-137-million-resolve-foreign-corrupt-practices-act.

[105] Press Release, U.S. Dep't of Justice, Fresenius Medical Care Agrees to Pay $231 Million in Criminal Penalties and Disgorgement to Resolve Foreign Corrupt Practices Act Charges (March 29, 2019), *available at* https://www.justice.gov/opa/pr/fresenius-medical-care-agrees-pay-231-million-criminal-penalties-and-disgorgement-resolve.

[106] Press Release, U.S. Dep't of Justice, Odebrecht and Braskem Plead Guilty and Agree to Pay at Least $3.5 Billion in Global Penalties to Resolve Largest Foreign Bribery Case in History (Dec. 21, 2016), *available at* https://www.justice.gov/opa/pr/odebrecht-and-braskem-plead-guilty-and-agree-pay-least-35-billion-global-penalties-resolve [hereinafter Odebrecht Press Release]. The $3.5 billion fine was paid to authorities in the United States, Brazil, and Switzerland. *Id.*

[107] *Id.*

[108] *Id.*

[109] Plea Agreement at 3, U.S. v. Odebrecht S.A., No. 16-643 (E.D.N.Y. Dec. 21, 2016).

[110] *Id.* at 4.

[111] *Id.* at 3.

Braskem also each agreed to retain independent compliance monitors for three years.[112] However, unlike Odebrecht, Braskem only received a 15 percent reduction in the fine range because of its less than full cooperation with the Justice Department.[113]

In certain cases, the DOJ has elected to charge only the *individuals* within the company involved in the wrongdoing, rather than the company itself, often based on the strength of the company's compliance program. One such example is the 2012 settlement of a FCPA case involving a former managing director of Morgan Stanley.[114] In April 2012, the employee pleaded guilty to corruption-related charges for his conduct in China.[115] In announcing this conviction, the government detailed all of the efforts made by Morgan Stanley to promote anti-corruption compliance and prevent such misconduct by its employees, including: publishing relevant and regularly-updated policies and procedures; providing frequent training, including 54 training programs for Asia-based personnel; training of the employee in question at least seven times, supplemented by 35 reminders about FCPA compliance; requiring periodic certifications of compliance with these policies by managers, including the individual in question; monitoring and random auditing of transactions and expenses; conducting extensive due diligence on all new business partners; and maintaining strict controls on payments to third parties.[116] Because Morgan Stanley "constructed and maintained a system of internal controls, which provided reasonable assurances that its employees were not bribing government officials," the DOJ declined to bring any enforcement action against the company.[117]

Similarly, in February 2019 the Justice Department declined to prosecute Cognizant, discussed *supra*, an American multinational corporation providing IT services, for its role in paying bribes to foreign officials.[118] Instead, the company's President and Chief Legal Officer were charged in a 12-count indictment with one count of conspiracy to violate the FCPA, three counts of violating the FCPA, seven counts of falsifying books and records, and one count of circumventing and failing to implement internal accounting controls.[119] On its decision not to prosecute the organization, the government pointed to, among other things, the company's thorough and comprehensive investigation, its full and proactive cooperation in the matter, the existence and effectiveness of its pre-existing compliance program, steps it took to enhance that

---

[112] *Id.* at 4.

[113] Plea Agreement at 5, U.S. v. Braskem S.A., No. 16-644 (E.D.N.Y. Dec. 21, 2016).

[114] Press Release, Former Morgan Stanley Managing Director Pleads Guilty for Role in Evading Internal Controls Required by FCPA (Apr. 25, 2012), *available at* https://www.justice.gov/opa/pr/former-morgan-stanley-managing-director-pleads-guilty-role-evading-internal-controls-required.

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] Letter from Craig Carpenito, *supra* note 80.

[119] Indictment of Gordon J. Coburn and Steven Schwartz, United States v. Gordon J. Coburn and Steven Schwartz (No. 19-120 KM), *available at* https://www.justice.gov/opa/press-release/file/1132691/download.

program and its internal accounting controls, and its timely and voluntary self-disclosure, which allowed the DOJ to investigate and identify the culpable individuals.[120]

These cases demonstrate that a company can avoid prosecution altogether by implementing an effective compliance program. Specifically, the efforts undertaken by Morgan Stanley and outlined by the government in that case offer a road map for a compliance program that can withstand the scrutiny of the Justice Department.

[2] SEC

[a] Seaboard Report and Its Progeny

In 2002, the SEC responded to one of the most prominent corporate frauds of the era—WorldCom—by obtaining a permanent injunction requiring the company to secure an independent review of its "corporate governance systems, policies, plans and practices" including "whether WorldCom has an adequate and appropriate code of ethics and business conduct, and related compliance mechanisms."[121] In addition to this requirement, the federal judge overseeing the securities fraud case against WorldCom ordered the company to train employees on business ethics and required that a sworn "Ethics Pledge" be signed by the Chief Executive Officer. The company then agreed to extend the pledge requirement to others in senior management and ultimately to all employees.[122]

Similarly, in 2003, the SEC reacted to the mutual fund scandals with a final rule requiring that all registered investment companies adopt a code of ethics, including comprehensive written policies and procedures designed to prevent violations of federal laws and regulations. These organizations must also appoint or designate a compliance officer to implement and help enforce these policies and procedures:

> We urge advisors to take great care and thought in preparing their codes of ethics, which should be more than a compliance manual. Rather, a code of ethics should also set out ideals for ethical conduct premised on fundamental principles of openness, integrity, honesty and trust. A good code of ethics should effectively convey to employees the value the advisory firm places on ethical conduct, and should challenge employees to live up not only to the letter of the law, but also to the ideals of the

---

[120] Letter from Craig Carpenito, *supra* note 80.

[121] SEC Litigation Release No. 17866 (Nov. 26, 2002); Accounting and Auditing Enforcement Release No. 1678 (Nov. 26, 2002).

[122] *See* Securities and Exchange Commission v. WorldCom, Inc., 273 F. Supp. 2d 431, 433 (S.D.N.Y. 2003). This requirement was reflected in the Corporate Monitor's final report, which also included the following recommendation: "The Company should commit to the highest standards of excellence in its ethics programs generally, and to the operation of a strong and effective Ethics Office within the management structure. The leadership of the Ethics Office should be someone with a very substantial level of legal experience, ideally including direct regulatory or law enforcement experience. The board should review all ethics programs thoroughly not less than annually, and should receive regular updates on the nature of issues that may arise." *See* Restoring Trust, Recommendation, Report of Richard C. Breedon (Oct. 2003), Recommendation 10.04, at p. 142.

organization.[123]

On October 23, 2001, the SEC issued an influential document—the so-called 21(a) Report in the *Seaboard* case.[124] This report explained why the SEC was taking enforcement action against the former controller of a public company's subsidiary, but *not* taking action against the public company itself. The SEC noted that "self-policing, self-reporting, remediation and cooperation with law enforcement" are "unquestionably important in promoting investors' best interests." It then detailed 13 criteria that the agency will consider in determining whether to bring charges and, if so, the *severity* of charges brought and sanctions to be sought. Among these criteria are the extent of the harm, the level of personnel involved, the immediacy and effectiveness of the company's response to the misconduct, and the timeliness and completeness of its notification to and cooperation with regulators. Moreover, regulators must ask if the company has adopted "new and more effective internal controls and procedures designed to prevent a recurrence of the misconduct?"

The Seaboard report has become a must-read for corporate counsel and compliance officers confronted with allegations of misconduct and a road map for how their organizations should respond to these allegations in an effort to avoid the most damaging outcomes.

In a significant, related development, the SEC on January 4, 2006, issued a "Statement of the Securities and Exchange Commission Concerning Financial Penalties."[125] The statement was released to "provide the maximum possible degree of clarity, consistency, and predictability" in the Commission's exercise of its authority to punish organizations for violations of federal securities laws and regulations. Among the factors that the SEC will consider are whether the organization has taken any remedial steps and the extent of the company's cooperation with the regulators: "The degree to which a corporation has self-reported an offense, or otherwise cooperated with the investigation and remediation of the offense, is a factor that the Commission will consider in determining the propriety of a corporate penalty." In one contemporaneous example, the SEC charged six former officers of a financial institution with fraud but not the institution itself because of the company's "swift, extensive and extraordinary cooperation." This cooperation included "prompt self-reporting, an independent internal investigation, sharing the results of that investigation with the government [without asserting applicable privileges], terminating and otherwise disciplining responsible wrongdoers, providing full restitution to its defrauded clients, and implementing new controls designed to prevent the recurrence of fraudulent conduct."[126]

---

[123] *See* SEC Final Rule: Investment Advisor Codes of Ethics [Release no. IA-2256, IC-26492; File No. S7-04-04] (July 2, 2004), at 4.

[124] Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions, SEC Release No. 34-44969 (Oct. 23, 2001), *available at* http://www.sec.gov/litigation/investreport/34-44969.htm.

[125] *Available at* www.sec.gov.

[126] SEC Litigation Release No. 19517, January 3, 2006.

This policy statement has been the subject of fierce debate regarding the appropriateness and scope of corporate versus individual penalties. In the course of this debate, SEC commissioners and staff have offered their views on the value of organizational compliance efforts. Then-Commissioner Luis Aguilar has suggested that, in determining whether a corporate penalty is warranted, regulators should consider "[t]o what degree was the company's culture respectful of the law, on the one hand, or driven to achieve particular results, on the other hand? Did the company have appropriate policies and procedures reflecting best practices for its size, business, and other circumstances? Was the board vigilant in overseeing management and steering the company?" He added his confidence "that companies can design efficient systems of compliance if properly motivated."[127]

In 2010, the SEC announced its intention to extend the benefits of cooperation to individuals as well as to organizations, by adopting a "Seaboard" plan for cooperating witnesses, complete with formal, written cooperation agreements. The Commission also has adopted some of the tools commonly used by the DOJ to encourage and reward self reporting and remediation, analogous to deferred prosecution and non-prosecution agreements (discussed below) with individuals and companies to postpone or eliminate enforcement action in return for full cooperation and the implementation of strengthened compliance programs and other controls.[128]

[b] Protections for Whistleblowers

[i] *Overview of Whistleblower Protections*

The Sarbanes-Oxley Act and the Dodd-Frank Act incorporate whistleblower protections as a means of incentivizing and protecting corporate insiders who may have information on corporate wrongdoing. As a result of these regulatory developments, corporate whistleblowers are an increasingly common phenomenon. In turn, anonymous reporting and anti-retaliation provisions are increasingly common aspects of corporate compliance programs.

[ii] *Sarbanes-Oxley Whistleblower Framework*

The Sarbanes-Oxley Act ("SOX") was enacted in 2002 in response to corporate and accounting scandals at Enron and other major corporations. In addition to promoting accountability, transparency, and fair markets, key provisions of SOX sought to encourage and protect corporate whistleblowers.

Section 301 of SOX requires that public company audit committees establish procedures for "the receipt, retention, and treatment" of complaints or other concerns—from any source—about auditing, internal controls and accounting matters, and for the

---

[127] Speech by Commissioner Luis A. Aguilar, "Reinvigorating the Enforcement Program to Restore Investor Confidence," March 18, 2009, *available at* http://www.sec.gov/news/speech/2009/spch031809laa.htm.

[128] *See, e.g.*, Robert S. Khuzami, Remarks at News Conference Announcing Enforcement Cooperation Initiative and New Senior Leaders (Jan. 13, 2010), *available at* https://www.sec.gov/news/speech/2010/spch011310rsk.htm.

"confidential anonymous submission by employees" of concerns about these issues.[129] Organizations may use their codes of conduct to publicize to both employees and external audiences the availability of special telephone lines and other communications vehicles for this purpose.

Section 806 creates a remedy for employees of public companies who believe they have suffered retaliation for providing information to the authorities, or otherwise assisting in the investigation of securities violations and other federal frauds. This section is enforced by the United States Department of Labor or by civil lawsuits in the federal courts.[130] The Department of Labor assigned its responsibility to the Occupational Safety and Health Administration ("OSHA"), which administers several other whistleblower statutes for the federal government.

The scope and protections available to whistleblowers under Section 806 have varied since its implementation, but three key points have remained consistent. First, the employee's allegations need not be correct to trigger whistleblower protections. Second, the reported legal violations covered by this section are not limited to those violations involving accounting fraud and financial reporting by public companies. Whistleblowers are also protected for complaints involving possible violations of securities, bank, mail or wire fraud laws, as well as "any rule or regulation of the Securities and Exchange Commission, or any provision of federal law relating to fraud against shareholders."[131] Lastly, the consequences to organizations that lose whistleblower cases can be quite significant. OSHA or the courts can order reinstatement, back-pay and any other relief required to make the employee "whole"—including damages for emotional distress—as well as attorney's fees and litigation costs.[132]

[iii] *Dodd-Frank's Whistleblower Framework*

[A] Overview of Dodd-Frank Whistleblower Protections

In 2010, Congress passed the Dodd-Frank Wall Street and Consumer Protection Act ("Dodd-Frank") in response to the financial crisis of 2008. The Act ushered in a new wave of significant financial regulation, primarily by the SEC, including key provisions aimed at incentivizing whistleblowers and protecting them from workplace retaliation.[133]

---

[129] Sarbanes-Oxley Act § 301, 15 U.S.C. § 78j-1(m)(4).

[130] Sarbanes-Oxley Act § 806, 18 U.S.C. § 1514A. Whistleblowers must, however, exhaust their administrative remedies in front of OSHA before a federal court may hear the claim. *See* 18 U.S.C. § 1514A(b)(1)(A)-(B*)*; *see also, e.g*., Wong v. CKX, Inc., 890 F. Supp. 2d 411, 417 (S.D.N.Y. 2012) ("A federal court may not hear a Sarbanes-Oxley claim that is not first submitted to OSHA and can only conduct de novo review of those Sarbanes-Oxley claims that have been administratively exhausted." (citation omitted)).

[131] Sarbanes-Oxley Act § 806(a), 18 U.S.C. § 1514(a)(i).

[132] *See* Bechtel v. Competitive Tech., 369 F. Supp. 2d 233 (D. Conn. 2005); Opinion & Order Re: Motion to Dismiss Plaintiffs' Complaint at 11–12, Feldman-Boland v. Morgan Stanley, No. 15-cv-06698-WHP (S.D.N.Y., July 13, 2016), ECF No. 37.

[133] Dodd-Frank Act, § 922(a) (2012).

The SEC has taken steps to entrench whistleblower protections by closely examining corporate policies that deter or undermine the free flow of information between employees and the Commission.

The Dodd-Frank Act amended the Securities and Exchange Act of 1934 by adding Section 21F, titled "Securities Whistleblower Incentives and Protection" and commonly referred to as the whistleblower provisions. This section defines a whistleblower as "any individual who provides, or 2 or more individuals acting jointly who provide, information relating to a violation of the securities laws to the Commission, in a manner established, by rule or regulation, by the Commission."[134]

Dodd-Frank's whistleblower reforms enhanced SOX whistleblower protections in important respects. In addition to the bounty and anti-retaliation provisions, both of which are discussed in more detail below, Dodd-Frank expands the whistleblower protections available under SOX in several ways. The Act provided a private right of action in federal court for whistleblowers facing retaliation, whereas SOX requires whistleblowers to first exhaust administrative remedies before turning to a federal court.[135] Next, Dodd-Frank specifically encompasses the actions of private subsidiaries and affiliates, while SOX only covered publicly traded companies at the time of its enactment.[136] Third, Dodd-Frank increases the statute of limitations for whistleblowers to report a violation for up to six years following the alleged retaliation, whereas SOX provides for a 180-day statute of limitations.[137]

Additionally, Dodd-Frank empowered the SEC to create the Office of the Whistleblower, which administers the SEC's Whistleblower Program.[138] To receive an award, a whistleblower must provide information that is both voluntary and original. The SEC considers a disclosure voluntary if it takes place before a formal request from the SEC.[139] The SEC considers information original if it is: (a) derived from independent knowledge; (b) not known to the SEC from any other source; (c) not exclusively derived from an allegation made in a judicial or administrative hearing, in a governmental report, hearing, audit or investigation, or from the news media, unless the whistleblower is the source of information; and (d) provided to the SEC for the first time after July 21, 2010.[140]

As of July 2019, the Office of the Whistleblower has approved whistleblower awards in connection with 48 covered actions, and has rejected 110 applications,[141] resulting

---

[134] Securities Whistleblower Incentives and Protection, § 21F (2012).

[135] *Id.*

[136] *Id*.

[137] *Id.*

[138] Welcome to the Office of the Whistleblower, Office of the Whistleblower, U.S. Securities and Exchange Commission, https://www.sec.gov/whistleblower/.

[139] Frequently Asked Questions, Office of the Whistleblower, U.S. Securities and Exchange Commission, https://www.sec.gov/about/offices/owb/owb-faq.shtml#P5_1383.

[140] *Id*; 17 C.F.R. § 240.21F-4(b)(4)(i)–(ii).

[141] Final Orders of the Commission, Office of the Whistleblower, SEC (last visited July 2, 2019),

in a roughly 30 percent award rate for whistleblowers. From the Office's inception through the end of Fiscal Year 2018, the SEC awarded $326 million to whistleblowers.[142] In Fiscal Year 2018 alone, the SEC awarded over $168 million in awards to 13 individuals, an amount exceeding the total amount awarded to whistleblowers in all previous years combined.[143] Awards vary significantly in amounts. In 2018, the SEC awarded the two highest bounties from single covered actions: $83 million to three individuals in March 2018 and $54 million to two individuals in September 2018. In addition to increasing award amounts, tips to the SEC have also increased. In Fiscal Year 2018, the SEC received over 5,200 whistleblower tips, the highest increase in tips since the beginning of the program in 2012.

[B] Dodd-Frank's Bounty Provisions

Dodd-Frank's bounty provision is one means of incentivizing possible whistleblowers to come forward with information to the Commission. Specifically, the Act establishes that the "Commission shall pay awards to eligible whistleblowers who voluntarily provide the SEC with original information that leads to a successful enforcement action."[144] Unlike Sarbanes-Oxley, which allows the SEC to use its discretion in determining whistleblower awards, Dodd-Frank mandates that the SEC provide whistleblowers with a share of between 10% and 30% of monetary sanctions ultimately imposed by the Commission where the sanction exceeds $1 million.[145]

[C] Dodd-Frank's Anti-Retaliation Provisions and Developments under *Digital Realty Trust*

Under the Dodd-Frank anti-retaliation provision, employers may not "discharge, demote, suspend, threaten, harass . . . or in any other manner discriminate" against a whistleblower where the whistleblower: (i) provides information to the SEC; (ii) initiates, testifies in, or assists with any investigation or action of the SEC; or (iii) makes disclosures required under the Sarbanes-Oxley Act, the Securities Exchange Act of 1934, and any other law, rule or regulation under the jurisdiction of the SEC.[146] Further, Dodd-Frank allows whistleblowers who experience retaliation to sue their employers directly in federal district court for reinstatement to their former position, double back pay plus interest, and compensation for litigation costs and attorneys' fees.[147]

Despite this seemingly broad retaliation protection, until recently, litigants and courts struggled to define the limits of this protection. The confusion largely stemmed from

---

https://www.sec.gov/about/offices/owb/owb-final-orders.shtml.

[142] 2018 Annual Report to Congress on the Dodd-Frank Whistleblower Program, U.S. Securities and Exchange Commission (Nov. 15, 2018), *available at* https://www.sec.gov/sec-2018-annual-report-whistleblower-program.pdf.

[143] *Id.*

[144] Whistleblower Program, U.S. Securities and Exchange Commission (last updated Aug. 12, 2011), *available at* https://www.sec.gov/spotlight/dodd-frank/whistleblower.shtml.

[145] *Id.*

[146] Dodd-Frank Act, § 922(h)(1)(A).

[147] Dodd-Frank Act, § 922(h)(1)(C).

subsection (iii) of Section 21F(h)(1)(A), described above, which incorporates anti-retaliation protection for required disclosures under Sarbanes-Oxley. As discussed, *supra*, Sarbanes-Oxley provides protections to internal reporters, seemingly creating a statutory conflict with Dodd-Frank's definition of a whistleblower in Section 21F(d)(6), which only protects whistleblowers who report directly to the Commission.[148] This confusion was heightened after the SEC promulgated Rule 21F-2(b) on whistleblower status and protection under Dodd-Frank. The first part of the rule defines a whistleblower as someone who provides *the Commission* with information. However, the second part of the rule provides retaliation protection to anyone who possesses a "reasonable belief" that the information he or she provides relates to a possible securities law violation and the information is provided in a manner described in clauses (i) through (iii) of § 922(h)(1)(A) of the act, "whether or not [the whistleblower] satisf[ies] the requirements, procedures and conditions to qualify for an award."[149] Therefore, under SEC Rule 21F-2, an individual could gain anti-retaliation protection under Dodd-Frank as a "whistleblower" without ever providing information to the SEC.

The Supreme Court resolved the conflict in its 2018 ruling in *Digital Realty Trust, Inc. v. Somers*, holding that Dodd-Frank's anti-retaliation provision only extends to an individual who has reported a violation of the securities laws to the SEC, not to one who made a purely internal report.[150] The Court held Dodd-Frank's definition of a "whistleblower," which requires individuals to report to the Commission, unambiguously applies to the act's anti-retaliation provision, and Congress's objective in passing the law, to "encourage SEC disclosures," supports such a reading.[151] The Court also held that Dodd-Frank's definition of whistleblower precluded the SEC from more expansively interpreting the term in Rule 21F-2.[152] Under the Court's ruling in *Digital Realty*, the Dodd-Frank retaliation provision stills protects whistleblowers who report internally so as long as "they also provide relevant information to the Commission."[153]

[iv] *Corporate Practices Seen as Deterring Whistleblowers*

In recent years, the SEC has focused on curbing corporate practices it perceives as deterring or impeding employees from reporting wrongdoing to the Commission. In particular, Rule 21F-17 prevents companies from "tak[ing] any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement . . . with respect to such communications."[154] Beginning in April 2015, the SEC initiated a series of enforcement orders against companies that violated Rule 21F-17, typically through improper language in confidentiality or severance agreements.

---

[148] 17 C.F.R. § 240.21F-4(b)(4)(i)–(ii).

[149] 17 CFR 240.21F-2.

[150] *Digital Realty Trust, Inc. v. Somers*, 138 S.Ct. 767, 772 (2018).

[151] *Id.* at 777, 780.

[152] *Id.* at 782.

[153] *Id.* at 780 (emphasis in original omitted).

[154] 17 C.F.R. § 240.21F–17.

The Commission brought the first of these enforcements against KBR, Inc. ("KBR") in 2015.[155] In *In the Matter of KBR, Inc.*, the SEC issued a cease and desist order against KBR for KBR's use of confidentiality agreements in its internal investigations that contained language violating Rule 21F-17.[156] The language at issue in the confidentiality agreements prohibited employees from discussing the internal investigations interview, or its subject matter, without prior authorization from KBR's law department.[157] Furthermore, the agreement stated that any such disclosures were "grounds for disciplinary action up to and including termination of employment." The SEC found that these provisions in the confidentiality agreement impeded the free flow of information regarding misconduct between employees and the Commission.[158] Although there was no evidence that the confidentiality agreement ever prevented an employee from communicating with the SEC, KBR agreed to (i) amend its confidentiality statement, (ii) make reasonable efforts to contact employees in the US who signed the agreements and inform them they are not required to seek permission before communicating with any governmental agencies, and (iii) pay a $130,000 penalty.[159]

In a similar enforcement action in August 2016, the SEC issued a cease and desist order against Health Net, Inc. ("Health Net") for language contained in its severance agreements.[160] Notably, Health Net had amended language in the severance agreements after the SEC adopted Rule 21F-17; however, the amended language specified that, while not prohibited from participating in an investigation, employees who executed the severance agreement's waiver and release of claims were prohibited from accepting a whistleblower award from the SEC.[161] Similar to KBR, Health Net agreed to amend its agreements, make reasonable efforts to contact former employees who signed the severance agreement, and pay a $350,000 fine.[162] From 2015 through 2017, the SEC charged a total of eight companies, including KBR and Health Net, with similar violations of Rule 21F-17.[163]

---

[155] *In the Matter of KBR, Inc*., Exchange Act Release No. 74619 (April 1, 2015).

[156] *Id.*

[157] *Id.*

[158] *Id.*

[159] *Id.*

[160] *In the Matter of Health Net, Inc.*, Exchange Act Release No. 78590 (August 16, 2016).

[161] *Id.*

[162] *Id.*

[163] *See In the Matter of Blue Linx Holdings Inc.*, Exchange Act Release No. 78528 (August 10, 2016); *In the Matter of Anheuser-Busch InBev SA/NV*, Exchange Act Release No. 78957 (September 28, 2016); *In the Matter of NeuStar, Inc.*, Exchange Act Release No. 79593 (December 19, 2016); *In the Matter of SandRidge Energy Inc.*, Exchange Act Release No. 79607 (December 20, 2016); *In the Matter of Black Rock, Inc.*, Exchange Act Release No. 79804 (January 17, 2017); *In the Matter of HomeStreet, Inc. and Darrell Van Amen*, Exchange Act Release No. 79844 (January 19, 2017).

[c] Recent SEC Resolutions

Similar to the DOJ enforcement actions, SEC deferred prosecution and non-prosecution agreements and other enforcement resolutions provide helpful insight into how the SEC views corporate compliance programs.

The SEC entered into its first deferred prosecution agreement on May 17, 2011, with Tenaris S.A. for FCPA violations.[164] The SEC allowed for a deferred prosecution agreement because Tenaris self-reported the violations upon discovery and subsequently strengthened its anti-corruption policies and procedures.[165] In an order announced on February 9, 2011, in a case involving ArthroCare Corporation, the SEC elaborated on the level of cooperation and the type of compliance program it expects to see in return for more lenient treatment.[166] The company regularly updated the SEC on its internal investigation; routinely granted the SEC staff access to its employees and consultants; replaced its senior management team; expanded its internal legal staff; created a new compliance department led by an experienced compliance professional; instituted quarterly ethics communications from senior management to employees; and provided regular compliance training.[167]

In June 2016, the SEC announced two non-prosecution agreements with Akamai Technologies and Nortek Inc., for similar, but unrelated matters involving bribes paid to Chinese officials.[168] In the respective agreements, the SEC noted that both companies had inadequate internal accounting controls and inaccurate books and records.[169] Nevertheless, the SEC credited both companies for their self-disclosure, "immediate action," and "significant remedial measures."[170] Nortek and Akamai's remedial measures included: strengthening their respective anti-corruption policies; developing a Compliance Committee and appointing a Chief Compliance Officer to supervise implementation of policies and training; providing extensive mandatory, in-person and online compliance trainings to employees in appropriate languages; revising internal audit testing and protocols; implementing comprehensive due diligence processes for channel partners; and enhancing travel and expense control requirements.[171]

---

[164] Press Release, SEC, Tenaris to Pay $5.4 Million in SEC's First-Ever Deferred Prosecution Agreement (May 17, 2011), *available at* https://www.sec.gov/news/press/2011/2011-112.htm.

[165] *Id.*

[166] ArthroCare Corp., Exchange Act Release No. 63883 (Feb. 9, 2011).

[167] *Id.* at 4.

[168] Press Release, SEC, U.S. Dep't of Justice, SEC Announces Two Non-Prosecution Agreements in FCPA Cases (June 7, 2016), *available at* https://www.sec.gov/news/pressrelease/2016-109.html [hereinafter Akamai and Nortek Press Release].

[169] Non-Prosecution Agreement between the SEC and Akamai Technologies, Inc., June 7, 2016, [hereinafter Akamai NPA] and Non-Prosecution Agreement between the SEC and Nortek, Inc., June 7, 2016 [hereinafter Nortek NPA].

[170] Akamai NPA at Exhibit A ¶ 9; Nortek NPA at Exhibit A ¶ 10.

[171] Akamai NPA at Exhibit A ¶¶ 9-10; Nortek NPA at Exhibit A ¶¶ 10-11.

Although Nortek and Akamai agreed to pay disgorgement and interest on their ill-gotten gains (approximately $320,000 and $670,000, respectively), both companies avoided paying any additional fines.[172] These two cases demonstrate the kind of favorable treatment a company may receive from the SEC for strengthening its compliance program and cooperating with the government. As the then-Chief of the SEC Enforcement Division's FCPA Unit stated, "Akamai and Nortek each promptly tightened their internal controls after discovering the bribes and took swift remedial measures to eliminate the problems. They handled [the misconduct] the right way and got expeditious resolutions as a result."[173] As discussed earlier in the chapter, Akamai and Nortek also received credit for their actions from the DOJ, which declined to prosecute under the FCPA Pilot Program.[174]

Similarly, on July 11, 2016, the SEC settled FCPA charges against Johnson Controls, Inc. ("JCI") for improper payments made by its Chinese subsidiary to employees of Chinese government-owned shipyards.[175] JCI's Chinese subsidiary, China Marine, had previously settled FCPA charges with the SEC in 2007 before it was acquired by JCI.[176] In an attempt to prevent further violations, JCI instituted several remedial measures including limiting the use of agents in its business model, hiring additional compliance personnel and conducting compliance trainings.[177] However, despite these efforts, the subsidiary was able to circumvent JCI's "less rigorous" internal controls through a sham vendor scheme and continued making improper payments to Chinese officials.[178] Although JCI ultimately failed to prevent the improper conduct, the SEC credited the company for its remedial efforts, compliance program and cooperation.[179] The Commission elected not to charge JCI with any violations, but instead issued a cease and desist order in which JCI agreed to pay $14 million in disgorgement and penalties to settle the charges.[180] Importantly, JCI neither admitted nor denied the allegations under the agreement, thereby reserving for itself the ability to contest any future litigation it may face as a consequence of the settlement.[181] As with Akamai and

---

[172] Akamai and Nortek Press Release.

[173] *Id.*

[174] *See* Letter from Daniel Kahn, Deputy Chief, Fraud Section, U.S. Dep't of Justice to Josh Levy, Counsel to Akamai Technologies, Inc.(June 6, 2016); *see* Letter from Daniel Kahn, Deputy Chief, Fraud Section U.S. Dep't of Justice to Luke Cadigan, Counsel to Nortek, Inc. (June 3, 2016).

[175] Johnson Controls, Inc., Exchange Act Release No. 78287 (July 11, 2016) [hereinafter JCI Cease and Desist].

[176] Press Release, SEC, Global HVAC Provider Settles FCPA Charges (July 11, 2016), *available at* https://www.sec.gov/litigation/admin/2016/34-78287-s.pdf [hereinafter JCI Press Release].

[177] *Id.*

[178] JCI Cease and Desist at 3–4.

[179] JCI Cease and Desist at 6.

[180] JCI Press Release.

[181] JCI Cease and Desist at 1.

Nortek, the DOJ recognized JCI's remedial efforts and settlement with the SEC and declined to prosecute JCI for the allegations.[182]

More recently, on April 23, 2018, the SEC settled charges against The Dun & Bradstreet Corporation for bribes paid by its employees in violation of the FCPA and its failure to maintain sufficient internal controls. These charges arose from improper payments made by two of the company's Chinese subsidiaries that were inaccurately recorded as lawful business expenses.[183] Dun & Bradstreet agreed to pay over $9 million in disgorged profits, interest and penalties without admitting or denying the allegations.[184] In evaluating the appropriateness of the settlement, the SEC considered Dun & Bradstreet's "self-disclosure, cooperation, and remedial efforts."[185] The DOJ subsequently declined to prosecute the company,[186] recognizing the company's cooperation with the SEC and "full remediation," which included strengthening internal compliance mechanisms, terminating the offending employees and disciplining others.[187]

Likewise, in December 2018, the SEC entered into a $16 million settlement with Polycom, Inc. for improper payments facilitated by its Chinese subsidiary. In its investigation, the SEC determined that the subsidiary encouraged "illicit payments to Chinese government officials in exchange for assistance in securing deals for Polycom products."[188] Although Polycom did not admit or deny the allegations,[189] the SEC cease and desist order credited the company's remedial measures, cooperation, and voluntary disclosure.[190] The DOJ declined to prosecute,[191] citing Polycom's cooperation with the SEC and its remedial steps to "enhance its compliance program and its internal accounting controls, terminat[e] the employment of 8 individuals involved in the misconduct, discipline[e] 18 other employees, and terminat[e] the Company's relationship with one of its channel partners."[192]

Notably, the SEC did not enter into any non-prosecution or deferred prosecution agreements in either 2017 or 2018. Nevertheless, the SEC continues to include them as

---

[182] Letter from Daniel Kahn, Deputy Chief, Fraud Section, U.S. Dep't of Justice to Jay Holtmeier, Counsel to Johnson Controls, Inc. (June 21, 2016).

[183] Press Release, SEC, SEC Charges Dun & Bradstreet with FCPA Violations (Apr. 23, 2018), *available at* https://www.sec.gov/enforce/34-83088-s.

[184] *Id*. *See also* Order, Dun & Bradstreet Corp., Exchange Act Release No. 83088 (Apr. 23, 2018) at 2.

[185] Order, Dun & Bradstreet Corp., Exchange Act Release No. 83088 (Apr. 23, 2018) at 7.

[186] *See* Letter from Sandra Moser, Acting Chief, Fraud Section, U.S. Dep't of Justice to Peter Spivack, Counsel to The Dun & Bradstreet Corporation (Apr. 23, 2018).

[187] *See id.*

[188] Press Release, SEC, SEC Charges Polycom, Inc. with FCPA Violations (Dec. 26, 2018), *available at* https://www.sec.gov/enforce/34-84978-s.

[189] *Id*. *See also* Order, Polycom, Inc., Exchange Act Release No. 84978 (Dec. 26, 2018) at 1.

[190] Order, Polycom, Inc., Exchange Act Release No. 84978 (Dec. 26, 2018) at 5.

[191] *See* Letter from Sandra Moser, Acting Chief, Fraud Section U.S. Dep't of Justice to Caz Hashemi and Rohan Virginkar, Counsel to Polycom, Inc. (Dec. 20, 2018).

[192] *See id.*

potential options for cooperative resolution in its Enforcement Manual.[193] Given that from 2012 to 2015 the SEC only issued approximately one NPA or DPA per year, this trend does not necessarily indicate that NPAs and DPAs will no longer play a significant role in SEC enforcement.

These cases demonstrate that prosecutors and regulators will continue responding to violations of law, in part, by mandating that organizations adopt and enforce compliance programs and, in particular, appropriate controls in the relevant areas of concern, or by giving credit to those organizations that have already done so. When companies prioritize compliance and in good faith attempt to combat unlawful behavior in their organizations, the government will typically endeavor to give them substantial credit for their efforts, despite the failure to completely eradicate the wrongdoing.

If, however, organizations fail to prioritize compliance, they may suffer the consequences. In 2012, Biomet Inc. entered into settlements with the DOJ and the SEC to resolve FCPA violations.[194] Under the settlements, Biomet agreed to pay over $17.28 million in criminal fines to the DOJ and $5.5 million in disgorgement and interest to the SEC.[195] The company also agreed to the appointment of an independent compliance monitor.[196] After the 2012 settlement, Biomet took steps to enhance its compliance program, including "conducting trainings, hiring additional compliance resources and implementing new policies and controls."[197] However, the company continued to interact, and improperly record transactions, with a prohibited distributor in Brazil and use a third-party customs broker to pay bribes to officials in Mexico.[198] As a result, on January 12, 2017, the SEC issued a cease and desist order against Zimmer Biomet, its successor company,[199] and the company entered into a new deferred prosecution agreement with the DOJ.[200] Under the SEC's order, Zimmer Biomet paid an additional $13 million in fines, disgorgement and interest to the SEC and agreed to retain an independent compliance monitor for an additional three-year period.[201] This case demonstrates the importance of developing more than a "paper" compliance program and the serious consequences a company may face if it fails to comply with the SEC and DOJ's settlement agreements.

In addition to the entity's liability, company officers and directors should be aware of potential liability they face personally when their organizations lack effective compli-

---

[193] *See* SEC, OFFICE OF CHIEF COUNSEL, ENFORCEMENT MANUAL §§ 6.2.2–6.2.3 (Nov. 28, 2017), *available at* https://www.sec.gov/divisions/enforce/enforcementmanual.pdf.

[194] Press Release, SEC, SEC Charges Medical Device Company Biomet with Foreign Bribery (March 26, 2012), *available at* https://www.sec.gov/news/press-release/2012-2012-50htm.

[195] *Id.*

[196] *Id.*

[197] Biomet, Inc., Exchange Act Release No. 79780 (Jan. 12, 2017) at 4.

[198] *Id.* at 4–7.

[199] Biomet Inc. was acquired by Zimmer Holdings in 2015 and renamed Zimmer Biomet.

[200] Press Release, SEC, Biomet Charged with Repeating FCPA Violations (Jan. 12, 2017), *available at* https://www.sec.gov/news/pressrelease/2017-8.html.

[201] Biomet, Inc., Exchange Act Release No. 79780 (Jan. 12, 2017) at 11.

ance programs. Under Section 20(a) of the Securities Exchange Act of 1934, which provides that anyone "who, directly or indirectly, controls any person liable" is also liable to the same extent as such controlled person, corporate executives can be held liable for the illegal acts of a foreign subsidiary, even absent allegations that the executives were personally complicit in the illicit conduct.[202] The SEC defines "control" as "the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract, or otherwise."[203]

Thus, in *SEC v. Nature's Sunshine Products* in 2009, the SEC settled with the company over the falsification of its books and records regarding its subsidiary's illicit cash payments to Brazilian customs officials and its subsequent creation of false documentation to cover up the payments.[204] In addition to charging the company, however, the SEC also charged the company's CEO and CFO as "control persons" for their failure to supervise direct reports who were responsible for keeping the books and records accurate and for putting in place sufficient internal controls to prevent the improper transactions, including two controllers who were aware that transactions were suspicious yet allowed them to be recorded as legitimate.[205] The corporate officers each paid a $25,000 civil penalty and agreed to an injunction against future violations of the books and records provision, even though there was no allegation that they knew of the improper payments, and the only linkage was their role in supervising the preparation of Nature's Sunshine's financial statements and maintaining the company's financial controls.[206]

Section 20(a), however, provides an affirmative defense where "the controlling person acted in good faith and did not directly or indirectly induce the act or acts constituting the violation or cause of action."[207] The Second and Ninth Circuits have interpreted "good faith" in this context to mean that "the controlling person must prove that he exercised due care in his supervision of the violator's activities in that he '*maintained and enforced a reasonable and proper system of supervision and internal control[s]*.' "[208] Companies are thus on notice that not even careful supervision of

---

[202] 15 U.S.C. § 78t.

[203] 17 CFR 230.405.

[204] Litigation Release No. 21162, SEC, SEC Charges Nature's Sunshine Products, Inc. with Making Illegal Foreign Payments (July 31, 2009), *available at* https://www.sec.gov/litigation/litreleases/2009/lr21162.htm.

[205] Compl. at 6–9, SEC v. Nature's Sunshine Products, Inc., No. 09-cv-00672-BSJ (D. Utah, July 31, 2009).

[206] *Id.* at 12–13; *see also* Litigation Release No. 21162, SEC, SEC Charges Nature's Sunshine Products, Inc. with Making Illegal Foreign Payments (July 31, 2009), *available at* https://www.sec.gov/litigation/litreleases/2009/lr21162.htm.

[207] 15 U.S.C. § 78t.

[208] SEC v. First Jersey Sec., Inc., 101 F.3d 1450, 1473 (2d Cir. 1996) (alteration in original) (emphasis added) (*quoting* Marbury Mgmt., Inc. v. Kohn, 629 F.2d 705, 716 (2d Cir. 1980)); *see also* Hollinger v. Titan Capital Corp., 914 F.2d 1564, 1576 (9th Cir. 1990) (a defendant "cannot satisfy its burden of proving

employees, standing alone, will protect top executives from "control person" liability under Section 20(a). Rather, the company must also "maintain[] and enforce[] a reasonable and proper" compliance system that will alert conscientious supervisors of any wrongdoing in the company, so that they can take the appropriate remedial measures.[209] Failure to create such a system leaves both the company and its officers at risk of prosecution.[210]

[3] Other Developments in the Evolution of Organizational Compliance Programs

[a] Growing Role of Independent Compliance Monitors

Over the past decade, corporate settlements with government agencies have increasingly included the appointment of independent compliance monitors. Under these settlements, the company and the prosecuting agency mutually agree to the appointment of an independent third party to assess and monitor the company's compliance with the terms of the settlement for a specified period of time. Monitorships allow corporations to benefit from the monitor's "expertise in the area of corporate

---

good faith merely by saying that it has supervisory procedures in place, and therefore, it has fulfilled its duty to supervise. A [defendant] can establish the good faith defense only by proving that it 'maintained and enforced a reasonable and proper system of supervision and internal control' " (*quoting* Zweig v. Hearst Corp., 521 F.2d 1129, 1134–35 (9th Cir. 1975))).

[209] *Hollinger*, 914 F.2d. at 1576.

[210] The U.S. Commodity Futures Trading Commission ("CFTC") has a similar control person provision requiring each CFTC registrant, "except an associated person who has no supervisory duties," to supervise diligently the handling "of all commodity interest accounts carried, operated, advised or introduced by the registrant and all other activities of its partners, officers, employees, and agents . . . relating to its business as a Commission registrant," *see* 17 C.F.R. 166.3. The CFTC relied on this provision to charge former Senator Jon S. Corzine with liability as a "control person" for his firm MF Global's "unlawful use of customer funds that harmed thousands of customers and violated fundamental customer protection laws on an unprecedented scale." *See* Press Release, CFTC, CFTC Charges MF Global Inc., MF Global Holdings Ltd., Former CEO Jon S. Corzine, and Former Employee Edith O'Brien for MF Global's Unlawful Misuse of Nearly One Billion Dollars of Customer Funds and Related Violations (June 27, 2013), *available at* http://www.cftc.gov/PressRoom/PressReleases/pr6626-13. The CFTC alleged that, "[i]n the summer and fall of 2011, as MF Global's need for cash was rising and its sources of cash were diminishing, Corzine knew that the firm was relying more and more on proprietary funds that it held alongside customer funds in FCM customer accounts. During this time, Corzine did not enhance MF Global's deficient systems and controls sufficiently to ensure that the firm's increasing reliance on FCM cash did not result in unlawful uses of customer money. Ultimately, these failures contributed to the massive customer losses." *Id.* Mirroring the standard set out by the Second and Ninth Circuits regarding 20(a) control person liability, the CFTC alleged that Corzine "held and exercised direct or indirect control over MF Global and Holdings and either did not act in good faith or knowingly induced these violations." Compl. at 3, CFTC v. MF Global Inc., et al., No. 13-CV-4463 (June 2, 2013), *available at* http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfmfglobalcomplaint062713.pdf. On January 5, 2017, the CFTC entered into a Consent Order against Corzine that found him liable for MF Global's violations as its controlling person. Under the order, Corzine was fined $5 million. Press Release, CFTC, Federal Court in New York Orders Jon S. Corzine to Pay $5 Million Penalty for his Role in MF Global's Unlawful Use of Nearly $1 Billion of Customer Funds and Prohibits Corzine from Registering with the CFTC in any Capacity or Associating with an FCM (Jan. 5, 2017) *available at* http://www.cftc.gov/PressRoom/PressReleases/pr7508-17.

compliance," and the corporation, its shareholders, employees and the public at large "benefit from reduced recidivism" of corporate misconduct and "the protection of the integrity in the marketplace."[211]

In 2008, the DOJ released guidance on the selection and use of monitors in its deferred prosecution and non-prosecution agreements. The "Morford Memorandum," authored by then-acting Deputy Attorney General Craig S. Morford, outlines nine principles related to independent corporate monitors.[212] The principles, summarized below, discuss the selection, scope of duties, and duration of compliance monitorships:

1. Qualifications: The monitor must possess the necessary qualifications based on the facts and circumstances of the case, and the monitor must be selected on the merits. The memorandum suggests that the monitor be selected from a pool of three qualified candidates.
2. Independence: A monitor is an independent third party, not an employee or agent of the corporation or the government.
3. Monitoring Compliance with the Agreement: The monitor's primary responsibility is to evaluate whether a corporation has both adopted and effectively implemented a compliance program to address and reduce the risk of the corporation's misconduct.
4. Scope: The monitor's responsibilities should be no broader than necessary to reduce the risk of recurrence of the corporation's misconduct.
5. Communications and Reports: The monitor may make periodic written reports to both the government and the corporation regarding the monitor's activities and the company's progress.
6. Reporting Adherence to the Monitor's Recommendations: If the corporation fails to adopt the recommendations made by the monitor within a reasonable time, either the monitor or the corporation, or both, should report that fact to the government, along with the corporation's reasons. The government may consider this conduct when evaluating whether the corporation has fulfilled its obligations under the agreement.
7. Reporting Previously Undisclosed or New Misconduct: The agreement should clearly identify any types of previously undisclosed or new misconduct that the monitor will be required to report directly to the government.
8. Duration: The duration of the monitorship should be tailored to the particular issues facing the corporation and the remedial measures needed in the particular case.
9. Extension or Early Termination: The agreement should provide for an

---

[211] C. Morford, Selection and Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations, *available at* https://www.justice.gov/usam/criminal-resource-manual-163-selection-and-use-monitors.

[212] *Id.*

extension of the monitor's term if the government determines the corporation has not successfully satisfied its obligations under the agreement. Conversely, the agreement should also provide for an early termination if the corporation demonstrates a change in circumstances sufficient to eliminate the need for a monitor.

In setting out these principles, the Justice Department sought to create a "practical and flexible" approach that takes into account "the varying facts and circumstances of each case."[213]

In 2010, the Justice Department supplemented the Morford Memorandum with the "Grindler Memorandum," named for then-acting Deputy Attorney General Gary G. Grindler.[214] The Grindler Memorandum added a tenth principle—that an agreement should explain the role the DOJ would play in resolving disputes that may arise between the monitor and the corporation. Through this last principle, the DOJ clarified that the Department's role in resolving disputes should be limited to determining whether the company has complied with the terms of the settlement agreement.[215]

In October 2018, the Justice Department released further guidance on when the imposition of independent compliance monitors is appropriate and on the selection of monitors.[216] The Morford Memorandum explained that when assessing the appropriateness of a monitorship, prosecutors should consider "(1) the potential benefits that employing a monitor may have for the corporation and the public, and (2) the cost of a monitor and its impact on the operations of a corporation."[217] The 2018 "Benczkowski Memorandum" elaborated on these two considerations with additional factors prosecutors should consider in evaluating the "potential benefits" of a monitor:

1. Whether the underlying misconduct involved manipulation of books or records, or "exploitation" of an existing but inadequate compliance program or internal controls;
2. Whether the underlying misconduct was "pervasive across the organization" or approved or facilitated by senior management;
3. Whether and the extent to which the corporation has made "significant investments in, and improvements to" its compliance program since the misconduct occurred;
4. Whether remedial improvements to the compliance program have been tested

---

[213] *Id.*

[214] G. Grindler, Additional Guidance on the Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations, *available at* https://www.justice.gov/usam/criminal-resource-manual-166-additional-guidance-use-monitors-dpas-and-npas.

[215] *Id.*

[216] B. Benczkowski, Selection of Monitors in Criminal Division Matters, *available at* https://www.justice.gov/opa/speech/file/1100531/download.

[217] C. Morford, Selection and Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations, *available at* https://www.justice.gov/usam/criminal-resource-manual-163-selection-and-use-monitors.

and demonstrate that they would prevent or detect similar misconduct in the future;

5. Whether there have been changes in the compliance environment and/or corporate leadership since the time of the misconduct, and if so, whether those changes are adequate to safeguard against a recurrence;
6. Whether there were adequate remedial measures taken to address problematic behaviors by employees or third parties, including termination of contributing business relationships or practices when appropriate; and
7. The unique risks and compliance challenges faced by the company including the region in which the company operates and the nature of the company's clientele.

The Benczkowski Memorandum also makes clear that prosecutors "should favor the imposition of a monitor only where there is a demonstrated need for, and clear benefit to be derived from, a monitorship relative to its projected costs and burdens." The Memorandum recognizes the importance of an effective compliance program to that decision: "Where a corporation's compliance programs and controls are demonstrated to be effective and appropriately resourced at the time of resolution, a monitor will likely not be necessary."

Although the principles set forth in the Morford, Grindler, and Benczkowski memoranda only directly apply to DOJ criminal proceedings against a corporation, the Justice Department and other governmental agencies have employed monitors in a wide range of cases.

For instance, in October 2016, a federal district judge appointed its own monitor over Deutsche Bank AG after the U.S. Commodities Futures Trading Commission sued the bank for failures of its swap data reporting system.[218] The court appointed the monitor to oversee the "implementation of appropriate measures for the generation of accurate, complete, and timely swap data reports by Deutsche Bank, as required by the [Commodity Exchange] Act and Regulations."[219]

In March 2017, the Federal Trade Commission agreed to the appointment of a monitor to oversee DaVita, Inc., a national outpatient kidney-dialysis chain.[220] The monitor oversaw the company's compliance with a settlement agreement resolving charges that DaVita's $358 million acquisition of a competitor was anti-competitive.[221]

---

[218] Martin O' Sullivan, *CFTC Wins Bid for Deutsche Bank Swaps-Reporting Monitor*, LAW360 (Oct. 20, 2016, 2:22 PM), *available at* https://www.law360.com/articles/853804/cftc-wins-bid-for-deutsche-bank-swaps-reporting-monitor.

[219] United States CFTC v. Deutsche Bank AG, No. 16-CV-6544, 2016 U.S. Dist. LEXIS 145479 at *4–5 (S.D.N.Y. Oct. 20, 2016).

[220] Press Release, FTC, FTC Requires Kidney Dialysis Chain DaVita, Inc. to Divest Assets as a Condition of Acquiring Competitor Renal Ventures Management LLC (Mar. 28, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/03/ftc-requires-kidney-dialysis-chain-davita-inc-divest-assets.

[221] *Id.*

Recently, additional federal judges and agencies have begun using independent monitors to compel corporate compliance. In March 2017, a federal district judge in Texas revised the terms of a plea agreement between the DOJ and the Chinese telecommunications company ZTE Corporation, reached after the company pled guilty to violating U.S. trade sanctions.[222] The judge appointed a compliance monitor to assess the company's adherence to export control laws.[223] The Department of Commerce reached a settlement with the company in June 2018, adding an additional federal monitor for a term of 10 years.[224] In October 2018, the district judge extended the original monitor's term and scope after finding that ZTE violated the terms of its probation by making false statements about disciplining employees involved in the sanctions violations.[225]

Even state regulatory agencies use independent compliance monitors. For instance, in 2016, the New York State Department of Financial Services required the Agricultural Bank of China and Mega International Commercial Bank of Taiwan to appoint monitors to settle anti-money laundering charges.[226] The monitors were appointed to "address serious deficiencies with the bank[s'] compliance program[s] and implement effective anti-money laundering controls."[227]

The DOJ has also begun using "hybrid" monitorships—a combination of an initial period of oversight from a traditional independent compliance monitor followed by a period of self-monitoring and reporting by the company.[228] In the past, the DOJ typically appointed monitors for a period of three years. However, recently in certain cases the DOJ has only required the company to use an independent monitor for the first 18 months of the term, with the company left to self-monitor and self-report for the

---

[222] Karen Freifeld, *U.S. Judge Says China's ZTE Violated Probation; Extends Monitor's Term* (Oct. 3, 2018), *available at* https://www.reuters.com/article/us-usa-trade-china-zte/u-s-judge-says-chinas-zte-violated-probation-extends-monitors-term-idUSKCN1MD2RX.

[223] Sue Reisinger, *In Rare Move, Judge Imposes Own Monitor in ZTE Plea Deal* (Mar. 29, 2017), *available at* https://www.law.com/corpcounsel/almID/1202782436926/.

[224] *See, e.g.*, Sue Reisinger, *US to Lift Export Ban on China's ZTE, Embed "Compliance Coordinators"*(June 7, 2018), *available at* https://www.law.com/corpcounsel/2018/06/07/u-s-to-lift-export-ban-on-chinas-zte-corp-embed-compliance-coordinators/.

[225] Karen Freifeld, *U.S. Judge Says China's ZTE Violated Probation; Extends Monitor's Term* (Oct. 3, 2018), *available at* https://www.reuters.com/article/us-usa-trade-china-zte/u-s-judge-says-chinas-zte-violated-probation-extends-monitors-term-idUSKCN1MD2RX.

[226] Press Release, N.Y.S. Dep't of Financial Services, DFS Fines Mega Bank $180 Million for Violating Anti-Money Laundering Laws (Aug. 19, 2016), *available at* http://www.dfs.ny.gov/about/press/pr1608191.htm [hereinafter Mega Bank Press Release]; Press Release, N.Y.S. Dep't of Financial Services, DFS Fines Agricultural Bank of China $215 Million for Violating Anti-Money Laundering Laws and Masking Potentially Suspicious Financial Transactions (Nov. 4, 2016), *available at* http://www.dfs.ny.gov/about/press/pr1611041.htm.

[227] Mega Bank Press Release, *supra* note 226.

[228] *See* Angela Xanakis, *The Future of FCPA Hybrid Monitorships*, LAW360 (May 15, 2014), *available at* https://www.law360.com/articles/538246?scroll=1.

remaining 18-month period.[229] Under these arrangements, the government reserves the right to extend the monitorship if the company fails to comply with the terms of its settlement.

Hybrid monitorships can result in significant cost savings for the company by allowing it to forgo the fees of an outside monitor for a significant portion of the settlement term. However, since the hybrid arrangements require self-monitoring and an inherent level of trust from the DOJ, so far the government has reserved them for settlements where the company has substantially cooperated with the government's investigation and undertaken remedial efforts.[230] For example, as discussed earlier in the chapter, Fresenius Medical, a dialysis equipment provider based in Germany, was recently offered a hybrid monitorship. The company voluntarily disclosed corruption and bribery schemes to the DOJ in 2012.[231] In March 2019, Fresenius signed a non-prosecution agreement that requires the company to retain an independent monitor for two years, then self-report for an additional year.[232]

If, during the course of the hybrid monitorship, the company fails to demonstrate its ability to self-monitor, the government can reinstitute the monitorship and even impose additional penalties. For example, as discussed earlier in the chapter, Biomet Inc. agreed to a hybrid monitorship with 18 months of independent monitoring and 18 months of self-reporting after settling with the SEC and DOJ over alleged FCPA violations in 2012.[233] However, after compliance issues persisted within the company, the government extended the length of the monitorship an additional year.[234] In 2017, Biomet entered into new settlements with the SEC and DOJ after discovering the misconduct had persisted even after the appointment of the first monitor in 2012.[235] Given Biomet's persistent problems, in the second round of settlements the government did not offer Biomet a hybrid monitorship option, and instead required the appointment of a new monitor for the full three-year term of the agreements.[236]

---

[229] For example in 2017, the DOJ entered a deferred prosecution agreement with Chilean chemical company Sociedad Quimica y Minera De Chile, S.A., allowing the company to use an independent monitor for the first two years and self-monitor for the last year of the term of the agreement. Deferred Prosecution Agreement between U.S. Dep't of Justice, Criminal Division and Sociedad Quimica y Minera De Chile, S.A., Jan. 13, 2017.

[230] Xanakis, *supra* note 228.

[231] Press Release, DOJ, Fresenius Medical Care Agrees to Pay $231 Million in Criminal Penalties and Disgorgement to Resolve Foreign Corrupt Practices Act Charges (Mar 29, 2019), *available at* https://www.justice.gov/opa/pr/fresenius-medical-care-agrees-pay-231-million-criminal-penalties-and-disgorgement-resolve.

[232] *Id.*

[233] Deferred Prosecution Agreement between U.S. Dep't of Justice Criminal Division and Biomet, Inc., Mar. 26, 2012.

[234] Biomet, Inc. (10-Q Quarterly Report) (Feb. 28, 2015).

[235] Press Release, SEC, Biomet Charged with Repeating FCPA Violations (Jan. 12, 2017), *available at* https://www.sec.gov/news/pressrelease/2017-8.html; *see also supra* 13.02[2][c].

[236] *Id.*

[b] ISO Compliance Standard

[i] *Overview of ISO 19600 Compliance Systems*

The International Organization for Standardization ("ISO") is an independent, non-governmental organization created in 1946, with its primary purpose "facilitat[ing] the international coordination and unification of industrial standards."[237] ISO has published international standards across many industries,[238] and develops standards based on distinct market needs.[239] ISO standards are based on "global expert opinion" and developed through "a multi-stakeholder process," including experts from the "relevant industry, consumer associations, academia, NGOs, and government."[240] Recently, ISO published international standards for organizations to use in establishing compliance and anti-bribery management systems.

[ii] *ISO 19600 Compliance Management Systems—Guidelines*

In 2014, ISO published ISO 19600:2014, "Compliance Management Systems—Guidelines," which provides guidance for "establishing, developing, implementing, evaluating, maintaining and improving an effective and responsive compliance management system."[241] The guidelines detail ways in which organizations can take steps to create effective compliance management systems in seven broad categories. These categories include:

1. Context of organization: identifying and evaluating compliance risks.[242]
2. Leadership: demonstrating a clear commitment to compliance management, and establishing a compliance policy that "is appropriate to the purpose of the organization; provides a framework for setting compliance objectives; includes a commitment to satisfy applicable requirements; [and] includes a commitment to continual improvement of the compliance management system."[243]
3. Planning: addressing compliance risks and creating compliance objectives.[244]
4. Support: providing resources, training, and open communication to support compliance management systems.[245]

---

[237] About ISO, International Organization for Standardization, *available at* https://www.iso.org/about-us.html (last visited July 26, 2017).

[238] *Id.*

[239] *Id.*

[240] How we Develop Standards, International Organization for Standardization, *available at* https://www.iso.org/developing-standards.html (last visited July 26, 2017).

[241] ISO 19600:2014, International Organization for Standardization, *available at* https://www.iso.org/standard/62342.html.

[242] Compliance Management Systems—Guidelines, ISO 5 (2014).

[243] *Id.* at 8.

[244] *Id.* at 13.

[245] *Id.* at 14.

5. Operation: establishing controls and procedures to meet compliance obligations.[246]
6. Performance Evaluation: monitoring, analyzing, and auditing the effectiveness of the compliance management system and the organization's performance.[247]
7. Improvement: correcting and managing noncompliance.[248]

These categories are "intended to be adaptable" depending on the "size and level of maturity of the organization's compliance management system and on the context, nature and complexity of the organization's activities, including its compliance and policy objectives."[249]

[iii] *ISO 37001 Anti-bribery Management Systems—Requirements with Guidance for Use*

In 2016, ISO published ISO 37001:2016, which focuses exclusively on anti-bribery management, and is "designed to help [organizations] combat bribery risk[s] in their own operations and throughout their global value chains."[250] In its Foreword to the standard, the ISO describes the destructive effects that bribery can have on social, political, and economic norms.[251] Further, the standard outlines the same seven steps found in ISO 19600 for establishing an effective anti-bribery management system and promoting a culture against bribery.[252]

Importantly, the standard allows organizations to become certified to ISO 37001 by ISO accredited third parties to "confirm that their anti-bribery management system meets the standard's criteria,"[253] and this dimension of the standard has received considerable attention from large corporations. In May 2017, Microsoft became the first company to announce that it would seek certification of its anti-corruption program under ISO 37001, after leading "the U.S. Technical Advisory Group of subject matter experts who authored [the] standard."[254] Microsoft was inspired to participate in the standard's development as one means of providing a consistent anti-corruption standard for companies operating around the world.[255] Walmart later announced that it too was

---

[246] *Id.* at 19.

[247] *Id.* at 21.

[248] *Id.* at 26.

[249] Introduction, Compliance Management Systems—Guidelines, ISO (2014).

[250] Elizabeth Gasiorowski-Denis, ISO Published Powerful New Tool to Combat Bribery, ISO (Oct. 14, 2016), *available at* https://www.iso.org/news/2016/10/Ref2125.html.

[251] Anti-bribery Management Systems—Requirements With Guidance For Use, ISO (2016).

[252] *Id.*

[253] Elizabeth Gasiorowski-Denis, ISO Published Powerful New Tool to Combat Bribery, ISO (Oct. 14, 2016), *available at* https://www.iso.org/news/2016/10/Ref2125.html.

[254] David Howard, An Update on Microsoft's Approach to Compliance, Microsoft on the Issue (May 7, 2017), *available at* https://blogs.microsoft.com/on-the-issues/2017/03/07/update-microsofts-approach-compliance/#sm.00006aokpc8o7erzpmm2fryp6u6en.

[255] Aarati Maharaj, Peeking Through the Windows, Ethisphere, *available at* http://insights.ethisphere.com/wp-content/uploads/Q2-2017-Peeking-Through-Microsoft.pdf.

considering getting certification under ISO 37001.[256] Walmart's announcement came after a lengthy FCPA-related investigation.[257] As of the 2019 update to this chapter, it is not evident that either has achieved this certification.

International companies have begun to pursue ISO 37001 certification more aggressively than organizations based in the United States. In 2017, French transportation company Alstom[258] and London-based IP company CPA Global[259] became certified. In 2018 and 2019, dozens more companies across the globe followed.[260] Some companies have pursued ISO 37001 certification after discovering past corruption in an effort to preemptively remedy the violations.[261] Recently, international enforcement agencies have begun to include ISO 37001 certification requirements as a requirement of bribery settlement agreements.[262]

[c] *Caremark*, Related Cases and Director Liability

[i] *The Caremark Case*

Whereas the FSGO made compliance programs an element of our criminal justice system, it was the *Caremark* decision[263] that brought compliance and codes of conduct into the boardrooms of American corporations. In what is widely regarded as a watershed case, the influential Delaware Chancery Court considered the responsibility of corporate directors to make sure that their organizations implement programs for legal and regulatory compliance. The court also addressed the personal liability of directors for failing to do so. Caremark, a healthcare company, had pleaded guilty to criminal fraud in 1995, in connection with allegations that it illegally paid doctors for patient referrals to Caremark facilities and violated other federal and state healthcare laws. The company paid $250 million in criminal fines and civil penalties.

One year later, the Delaware Chancery Court was asked to approve the settlement of a shareholder derivative suit alleging that the Caremark directors had breached their duty of care by failing to prevent the fraud by the company's employees. The suit sought reimbursement to the company of the fines and penalties, but the settlement did

---

[256] Kevin Krolicki, Wal-Mart Seeks Anti-Corruption Certification, in Talks With Regulators, Reuters (May 3, 2017), *available at* http://www.reuters.com/article/us-usa-compliance-walmart-idUSKBN17Z2PM.

[257] *Id.*

[258] Alstom Joins the Ranks of ISO 37001-Certified Companies (July 11, 2017), *available at* https://create.org/news/alstom-joins-ranks-iso-37001-certified-companies/.

[259] Anna Oleary, CPA Global Achieves IOS 37001 Anti-Bribery Certification (July 13, 2017), *available at* https://www.cpaglobal.com/press-releases/cpa-global-achieves-iso-37001-anti-bribery-certification.

[260] Worth MacMurray, Three predictions for the future of ISO 37001 (Feb 13, 2019), *available at* http://www.fcpablog.com/blog/2019/2/13/three-predictions-for-the-future-of-iso-37001.html.

[261] *See* Vera Cherepanova, ISO 37001: Not all certifications are created equal (April 3, 2019), *available at* http://www.fcpablog.com/blog/2019/4/3/iso-37001-not-all-certifications-are-created-equal.html.

[262] MacMurray, *supra* note 260.

[263] *In re* Caremark Int'l Derivative Litig., 698 A.2d 959 (Del. Ch. 1996).

not provide such relief. The court approved the settlement, concluding that there was little likelihood that the directors in this case had "breached any duty to appropriately monitor and supervise the enterprise."[264]

At the same time, the court did not let corporate directors off the hook in regards to oversight of their organization's legal and regulatory compliance:

> [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, . . . [T]he failure to do so may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards.[265]

The goal of this system is "to provide to senior management and the Board itself timely, accurate information sufficient to allow management and the Board, each within its scope, to reach informed judgments concerning both the corporation's compliance with law and its business performance." The required system of information and reporting must be ongoing, so that it is "in concept and design adequate to assure the Board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility."[266]

The *Caremark* court specifically referred to the FSGO in connection with the kind of system that corporations should implement, noting that the Sentencing Guidelines "offer powerful incentives for corporations today to have in place compliance programs to detect violations of law, promptly to report violations to appropriate public officials when discovered, and to take prompt, voluntary remedial effort . . . Any rational person attempting in good faith to meet an organizational governance responsibility would be bound to take into account this development and the enhanced penalties and the opportunities for reduced sanctions that the federal sentencing guidelines offer."[267]

Moreover, in approving the settlement, the court favorably reviewed the compliance procedures that the company had adopted. These included:[268]

(1) Adoption and publication of a new ethics manual for employees that included a toll-free hotline for employees to confidentially report possible violations of law or company policy;

(2) New policies to prevent misconduct in government programs; and

(3) Establishment of an audit plan to test legal and regulatory compliance.

[ii] *Cases Related to Caremark*

Cases interpreting *Caremark* have admonished corporate directors that they breach their duty of care if they intentionally or recklessly disregard " 'red flags' that warned

---

[264] *Caremark*, 698 A.2d at 961.

[265] *Caremark*, 698 A.2d at 970.

[266] *Caremark*, 698 A.2d at 970.

[267] *Caremark*, 698 A.2d at 968–70.

[268] *Caremark*, 698 A.2d at 963–66.

of the systematic fraudulent practices employed and encouraged by . . . management."[269] In one case, the red flags included audit results, a whistleblower lawsuit, a federal investigation and a series of articles in the *New York Times* regarding a hospital company's billing practices.[270] In another case, the court found a "sustained and systematic failure of the Board to exercise oversight" when the Audit Committee of the Board of Directors "took no steps in an effort to prevent or remedy" the company's repeated and well-documented noncompliance with FDA requirements.[271] In a third case, the Delaware Chancery Court provided some examples that would constitute a failure to meet the *Caremark* standards: "That the company lacked an audit committee, that the company had an audit committee that met only sporadically and devoted patently inadequate time to its work, or that the audit committee had clear notice of serious accounting irregularities and simply chose to ignore them or, even worse, to encourage their continuation."[272]

Nonetheless, the Delaware Supreme Court has remarked that *Caremark* claims are "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment," and courts interpreting *Caremark* have limited the doctrine's reach.[273] In the absence of "red flags" that put them on notice of wrongdoing, directors are liable for breaching their duty of oversight under Delaware law only if (a) they "utterly failed to implement any reporting or information system or controls; *or* (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."[274] Thus, directors may discharge their duty of oversight, in appropriate circumstances, by ensuring that a company has an adequate compliance program and periodically receiving reports from the officers responsible for the operation of the program. "As numerous Delaware decisions make clear, an allegation that the underlying cause of a corporate trauma falls within the delegated authority of a board committee does not support an inference that the directors on that committee knew of and consciously disregarded the problem."[275] For example, the Delaware Chancery Court in *South v. Baker* found that "three mining incidents in a year [did] not support a reasonable inference of board involvement, much less bad faith, conscious wrongdoing, or knowing indifference," especially since the board had established a

---

[269] McCall v. Scott, 239 F. 3d 808, 819 (6th Cir. 2001).

[270] *See McCall*, 239 F.3d at 819.

[271] *In re* Abbott Labs. Derivative Litig., 325 F.3d 795, 809 (7th Cir. 2003).

[272] Guttman v. Huang, 823 A.2d 492, 507 (Del. Ch. 2003). *See also* American Int'l Group v. Greenberg, 965 A.2d 763, 801 (D. Ch. 2009) (denying, in part, motions to dismiss claims against certain director defendants when allegations of the complaint supported an inference that they were aware of "pervasive, earnings-related frauds").

[273] Stone v. Ritter, 911 A.2d 362, 372 (Del. 2006).

[274] *Id. See also In re* SFBC Intern. Inc., 495 F. Supp. 2d 477, 484–85 (D.N.J. 2007) ("lack of good faith can be established by a sustained or systematic failure of the board to exercise oversight").

[275] South v. Baker, 2012 Del. Ch. LEXIS 229, at *36 (Sept. 25, 2012).

Safety Committee that reviewed relevant policies, discussed material noncompliance with management and received updates from management on safety performance.[276]

In *Stone v. Ritter*, the Delaware Supreme Court affirmed the dismissal of a derivative action when it was clear from the face of the pleadings (including from a report incorporated by reference) that "the Board received and approved relevant policies and procedures, delegated to certain employees and departments the responsibility for filing [reports required under the Bank Secrecy Act] and monitoring compliance, and exercised oversight by relying on periodic reports from them."[277]

The Delaware Chancery Court also refused to second-guess the directors of Citigroup for allegedly failing to protect the organization and its shareholders from the risks of the sub-prime mortgage market.[278] The court explained that the "[o]versight duties under Delaware law are not designed to subject directors, even expert directors, to *personal liability* for failure to predict the future and to properly evaluate business risk."[279] The court noted that the plaintiffs had conceded that "Citigroup had a risk monitoring system in place."[280] The Delaware Supreme Court has held that, "officers of Delaware corporations, like directors, owe fiduciary duties of care and loyalty, and that the fiduciary duties of officers are the same as directors."[281]

In a case stemming from the 2008 financial crisis, the Delaware Chancery Court rejected an effort to extend directors' *Caremark* responsibilities, and potential liabilities, to the monitoring of business risk.

> The "unethical" conduct the Plaintiffs allege here, however, is not the type of wrongdoing envisioned by *Caremark*. The conduct at issue here involves, for the most part, *legal* business decisions that were firmly within management's judgment to pursue . . . . Legal, if risky, actions that are within management's discretion to pursue are not 'red flags' that would put a board on notice of unlawful conduct.[282]

Coupled with the strict pleading standards requiring "specific facts" to support the inference of director "bad faith, conscious wrongdoing, or knowing indifference,"[283] stating a *Caremark* claim can be difficult. A recent Chancery decision—cited favorably

---

[276] South v. Baker, 2012 Del. Ch. LEXIS 229, at *39–40 (Sept. 25, 2012).

[277] Stone v. Ritter, 911 A.2d 362, 373 (Del. 2006); *see also* Midwestern Teamsters Pension Trust Fund v. Deaton, 2009 U.S. Dist. LEXIS 50521 (S.D. Tex., May 27, 2009) (directors were not responsible for violations of the Foreign Corrupt Practices Act, even when committed by a company already under a cease and desist order for similar violations, because the board and the company had taken steps as part of its compliance program to comply with a prior order and prevent violations).

[278] *In re* Citigroup Shareholder Derivative Litig., 964 A.2d 106 (Del. Ch. 2009).

[279] *In re* Citigroup Shareholder Derivative Litig., 964 A.2d 106, 131 (Del. Ch. 2009) (emphasis in original).

[280] *In re* Citigroup Shareholder Derivative Litig., 964 A.2d 106, 129 (Del. Ch. 2009).

[281] Gantler v. Stephens, 965 A. 2d 695, 709 (Del. 2009).

[282] *In re* Goldman Sachs Group, Inc. S'holder Litig., 2011 Del. Ch. LEXIS 151 (Oct 12, 2011).

[283] TVI Corp. v. Gallagher, No. CV 7798-VCP, 2013 Del. Ch. LEXIS 260 (Del. Ch. Oct. 28, 2013); South v. Baker, 62 A.3d 1, 18 (Del. Ch. 2012).

by the Second Circuit[284]—has reiterated the importance to companies of having a compliance and reporting system in place, and how challenging it is for a plaintiff to assert a *Caremark* claim in the face of such a compliance program. The Chancery explained:

> Contentions that the Board did not receive specific types of information do not establish that the Board utterly failed "to attempt to assure a reasonable information and reporting system exists," particularly in the case at hand where the Complaint not only fails to plead with particularity that [the company] lacked procedures to comply with its . . . reporting requirements, but actually concedes the existence of information and reporting systems . . . .
>
> In other words, the Plaintiffs complain that [the company] could have, should have, had a *better* reporting system, but not that it had *no* such system.
>
> Stated more generally, in criticizing the Board's risk oversight and its delegation thereof, throughout the Complaint, the Plaintiffs concede that the Board was exercising *some* oversight, albeit not to the Plaintiffs' hindsight-driven satisfaction . . . . That is short of pleading that the Board "utterly failed to implement any reporting or information system or controls," sufficient to raise a reasonable doubt of the directors' good faith.[285]

That said, these types of cases are not so challenging for plaintiffs that companies have avoided settling them. For instance, in February 2018, the Chancery Court approved a $90 million settlement of a Twenty-First Century Fox derivative lawsuit in which shareholders alleged that the directors failed to monitor and respond to widespread instances and complaints of sexual harassment and racial discrimination.[286] The company also agreed as part of the settlement to institute a Workplace Professionalism and Inclusion Council for a term of five years.[287] The council, comprised of six members, will be responsible for monitoring harassment and discrimination within the company.[288] The agreement stipulates that the council has the power to recommend and conduct independent investigations into specific instances and hire outside consultants.[289] The council will also report to the board regularly and its findings shall be available to the public.[290]

---

[284] Central Laborers v. Dimon, No. 144516 (2d Cir. Jan. 6, 2016).

[285] *In re* General Motors Co. Derivative Litig., No. CV 9627-VCG, 2015 WL 3958724, at *14–15 (Del. Ch. June 26, 2015) (emphasis in original) (internal quotation marks omitted).

[286] *See City of Monroe Employees' Retirement System v. Murdoch et al*., No. 2017-0833 (Del. Ch. Nov. 20, 2017).

[287] Jeff Montgomery, Fox's "Unusual" $90M Scandal Deal Gets Chancery's OK (Feb. 19, 2018), *available at* https://www.law360.com/articles/1011154/fox-s-unusual-90m-scandal-deal-gets-chancery-s-ok.

[288] *Id*.

[289] Mark Lebovitch, Settlement of Workplace Harassment Suit at 21st Century Fox (Dec. 19, 2017), *available at* https://corpgov.law.harvard.edu/2017/12/19/settlement-of-workplace-harassment-suit-at-21st-century-fox/.

[290] *See id.*

Finally, suits brought under laws of jurisdictions other than Delaware have also alleged that directors breached their fiduciary duties by failing to implement and maintain internal controls against misconduct. For instance, a shareholder derivative action filed in May 2019 against Exxon Mobil, a New Jersey corporation, related to climate change, alleges, among other things, that its officers and directors breached their fiduciary duties under New Jersey law "to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the financial affairs of the [c]ompany."[291]

[iii] ***Additional Guidance on Director Liability***

A shareholder derivative suit under the challenging *Caremark* standard is not the sole avenue of liability that should concern directors. Of equal, if not greater, concern is enforcement by the government, particularly the SEC, which has repeatedly warned corporate directors that they will be held to an exacting standard of oversight given their roles as "gatekeepers." In an influential speech at the 2013 Securities Enforcement Forum, then-SEC Chairperson Mary Jo White put companies on notice that the SEC would begin "focusing on deficient gatekeepers—pursuing those who should be serving as the neighborhood watch, but who fail to do their jobs," and—striking fear in directors nation-wide—continued that "[i]nvestment company boards serve as critical gatekeepers and we will focus on ensuring that they appropriately perform their duties."[292] She then went on:

> It has been suggested that our focus on gatekeepers may drive away those who would otherwise serve in these roles, for fear of being second-guessed or blamed for every issue that arises. I hear and I am sensitive to that concern. But this is my response: first, being a director or in any similar role where you owe a fiduciary duty is not for the uninitiated or the faint of heart. And, second, we will not be looking to charge a gatekeeper that did her job by asking the hard questions, demanding answers, looking for red flags and raising her hand.[293]

Chairperson White returned to the topic of "gatekeeper" liability in a June 2014 speech in front of the Stanford Directors' College. White reiterated that "a company's directors serve as its most important gatekeepers" and clarified the SEC's expectations regarding directors' conduct *qua* "gatekeepers." Directors must "establish expectations for senior management and the company as a whole, and exercise appropriate oversight to ensure that those expectations are met." Specifically, directors have the "critical responsibility" of setting the appropriate "tone at the top" as well as "the standard in the boardroom that good corporate governance and rigorous compliance are essential." She then admonished directors that they "must ask the difficult questions, particularly if you see something suspicious or problematic, or, simply, when you do not understand,"

---

[291] Verified Shareholder Derivative Complaint, Colditz v. Woods, 3:19-cv-01067, Dkt. 1, at ¶ 314 (May 2, 2019). *See also id.* ¶ 349, Prayer for Relief ¶ B.

[292] Mary Jo White, Remarks at the Securities Enforcement Forum (Oct. 9, 2013), *available at* https://www.sec.gov/News/Speech/Detail/Speech/1370539872100.

[293] *Id.*

"should never ignore red flags," and must "be knowledgeable about issues, . . . vigilant in protecting against wrongdoing, and [must] tackle difficult issues head on."[294]

As Chairperson White and subsequent leaders of the SEC have acknowledged, however, enforcement actions against directors—particularly outside directors—are rare and have tended to involve circumstances where directors either "have taken affirmative steps to participate in fraudulent misconduct or have otherwise enabled fraudulent misconduct to occur by unreasonably turning a blind eye to obvious 'red flags' of misconduct."[295] Nonetheless, Chairperson White's remarks and more recent SEC warnings reflect an expectation that directors exhibit the same ethical standards that they expect from the rest of the company, and ensure not only that the company's compliance program contains appropriate methods for employee concerns and other significant issues to get accurately reported to the board in a timely fashion, but that the programs include mechanisms by which the company can appropriately respond to and remediate the issues.

§ 13.03 Developing an Effective Compliance Program

[1] Creating and Demonstrating a "Culture of Compliance"

Before turning to the task of drafting a new code of conduct or revising an existing one, corporate counsel and compliance officers should consider their organization's "culture of compliance." Increasingly, regulators are looking for evidence that an organization not only has the right process, but also that it has the right culture. As SEC Chairman Jay Clayton has stated, "[w]hile there is great importance in setting a positive 'tone at the top,' an organization's culture is, in large part, defined by the countless daily actions of its people. Culture is not just what is said by management to the work force, but what is done, i.e., what actions are taken, day in and day out throughout the organization."[1] In June 2018, he offered his observations on how financial institutions can drive positive culture:

> There are many familiar methods for communicating, monitoring and reinforcing cultural objectives—compliance programs, policies and procedures, training, personnel decisions (including evaluations and compensation), etc. I believe all of these methods are important and, in large financial organizations, essential. I also believe these methods are enhanced by, and in fact, to be effective over the long term, require, a clear,

---

[294] Mary Jo White, A Few Things Directors Should Know About the SEC (June 23, 2014), *available at* https://www.sec.gov/News/Speech/Detail/Speech/1370542148863.

[295] Commissioner Luis A. Aguilar, The Important Work of Boards of Directors (Oct. 14, 2015), *available at* https://www.sec.gov/news/speech/important-work-of-boards-of-directors.html; Mary Jo White, A Few Things Directors Should Know About the SEC (June 23, 2014), *available at* https://www.sec.gov/News/Speech/Detail/Speech/1370542148863. *See also* Bradley J. Bondi et al., *A Brief History Of SEC Enforcement Actions Against Directors*, Law360 (Oct. 16, 2015, 1:59 PM), *available at* http://www.law360.com/assetmanagement/articles/714967/a-brief-history-of-sec-enforcement-actions-against-directors (concluding that SEC actions against directors are "rare" and "have involved significant allegations of wrongdoing by directors").

[1] Jay Clayton, Chairman, SEC, Observations on Culture at Financial Institutions and the SEC (June 18, 2018), *available at* https://www.sec.gov/news/speech/speech-clayton-061818.

> candid, easily understandable articulation of the organization's core mission . . . . [A clear mission] fills in the gaps. Organizations with the most comprehensive compliance programs and policies and procedures will inevitably encounter circumstances not contemplated by their policies and procedures . . . . In these circumstances, those on the front lines, those making decisions, need a touchstone.[2]

In other speeches, officials at the DOJ and SEC have added substance and specificity to what might otherwise be an element that is impossible to evidence or measure. Andrew J. Donohue, then-Chief of Staff of the SEC, offered his perspective on the elements of a "culture of compliance" in a 2016 keynote speech at the Rutgers Law School Center for Corporate Law and Governance:[3]

- "[A] critical component of an effective corporate compliance program is the integrity of those people you have in your organization and their ownership of personal responsibility for themselves and the areas for which they are responsible."
- "A culture of always doing the right thing, not tolerating bad practices or bad actors is essential. The culture should encourage people to ask questions and to discuss openly what is the proper response to a particular issue and how conflicts should be resolved. It should hold the higher up members of the firm to at least the same standard of conduct as those below them."
- "Another sign of the culture of a firm is whether there is a correlation between ethical behavior and the firm's reward structure, such as salaries, bonuses and promotions."
- "When developing the policies and procedures you expect the firm and its personnel to follow they will be most effective if they are as simple as possible, are explained in plain English and are intuitive to those that have to comply with them."
- "It is not about assigning blame when a problem occurs but rather ensuring ownership of the process to lessen the likelihood that there will be a problem. This can be pervasive within an organization where technology has been employed extensively."
- "While you can segregate many tasks and responsibilities within a complex firm so they are manageable, you still need a number of key personnel who appreciate how it all works and can then identify where there may be gaps or inconsistencies."

---

[2] *Id.*

[3] Andrew J. Donohue, SEC Chief of Staff, Keynote Luncheon Speech at the Rutgers Law School Center for Corporate Law and Governance, New Directions in Corporate Compliance (May 20, 2016), *available at* https://www.sec.gov/news/speech/donohue-rutgers-new-directions-corporate-compliance-keynote.html.

Another measure of a company's compliance culture is how it responds to violations. Stephen L. Cohen, then-Associate Director of the SEC Enforcement Division, offered these suggestions for identifying and responding to compliance violations:[4]

- "Risk-taking in the area of legal and ethical obligations invariably leads to bad outcomes . . . Tolerating close-to-the-line behavior sends a terrible message throughout an organization that pushing the envelope is acceptable."
- "Be on the lookout for people who are overly technical in their approach to issues of ethics and professional responsibility. Pay particular attention to those who may disparage or diminish the importance of respect for the law and protecting the organization from reputational harm."
- "Be skeptical of explanations that don't add up regardless of who provides them. If someone explains something to you in a way that you don't understand, don't accept it."
- "[W]histleblowers who don't report internally repeatedly tell us that they believe they will be retaliated against if they raise significant issues to management . . . Companies must take active steps to address this perception."

Similarly, Brent Snyder, the then-Deputy Assistant Attorney General of the DOJ's Antitrust Division remarked in 2014 that, while there is no "one size fits all" answer for what makes an effective compliance program, there are some common principles that companies can call upon:[5]

- "First, it starts at the top. A company's senior executives and board of directors must fully support and engage with the company's compliance efforts."
- "Second, a company should ensure that the entire organization is committed to its compliance efforts and can participate in them. This means educating all executives and managers, and most employees."
- "Third, a company should ensure that it has a proactive compliance program. This means that in addition to providing training and a forum for feedback, a company should make sure that at risk activities are regularly monitored and audited."
- "Fourth . . . a company should be willing to discipline employees who either commit . . . crimes or fail to take the reasonable steps necessary to stop the criminal conduct in the first place."
- "Finally, a company that discovers criminal . . . conduct should be prepared to take the steps necessary to stop it from happening again. This likely includes making changes to a compliance program that failed to prevent the criminal conduct initially."

---

[4] Stephen L. Cohen, SEC Associate Director of Enforcement, Remarks at SCCE's Annual Compliance & Ethics Institute (Oct. 7, 2013), *available at* https://www.sec.gov/news/speech/spch100713slc.

[5] Brent Snyder, Deputy Assistant Attorney General in the DOJ Antitrust Division, Compliance is a Culture, Not Just a Policy (Sept. 9, 2014), *available at* https://www.justice.gov/atr/file/517796/download.

Research by the Ethics Resource Center indicates that creation and maintenance of the right ethics and compliance culture can have as much if not more favorable impact on an organization's compliance performance as the implementation of compliance processes and tools. In these organizations, where there is encouragement of internal reports, consistent responses to reported problems, and no tolerance for retaliation, employees are more likely to report misconduct and are less likely to experience retaliation or pressure to bend the rules.[6] Likewise, the Ethics Compliance Institute found that as compared to employees in weak ethics and compliance cultures, employees in strong cultures are 38% less likely to observe FCPA violations, 76% less likely to observe False Claims Act violations, and 65% less likely to observe other white collar crimes.[7] Companies that promote cultural integrity can thus reduce their compliance risks.

In short, an effective compliance program will effectively address these three issues:

1. Culture: it must promote and maintain a "culture of compliance";
2. Risk: it must identify and mitigate the most significant legal and regulatory compliance risks facing the organization; and
3. Leadership: its leaders must promote and be accountable for ethics and compliance.

Organizations may be held responsible for representations about their compliance program. For example, in a recent case involving Credit Suisse Group, the court refused to dismiss allegations of material omissions and misstatements about the company's risk management system and protocols, finding sufficient allegations that Credit Suisse repeatedly breached the limits of its own policies. The court stated that:

> [Credit Suisse] represented a comprehensive and multi-layered risk management system, involving "more than 100 individual risk limits," designed to "trigger" oversight in the event of a change in the risk profile . . . [T]he 2014 Annual Report devoted over thirty-five pages to describing [Credit Suisse's] "extensive risk protocols." Although the Annual Report repeatedly represented that risk limits were "binding" and no breaches occurred, the Complaint identifies at least three instances when the limits were not binding and effectively breached. The Complaint sufficiently pleads materially misleading statements and omissions about [Credit Suisse's] risk limits and controls.[8]

No company can achieve the fundamental objectives of an effective compliance program without the right code of conduct, which will then serve as both the foundation and the support for the compliance culture and processes in an organization. This is the topic of discussion in the next section.

---

[6] The State of Ethics and Compliance in the Workplace (2018), Ethics & Compliance Initiative, *available at* https://www.ethics.org/knowledge-center/eci-recent-research/.

[7] *See* "EthicsStats July 2018," Ethics & Compliance Initiative (2018), *available at* https://www.ethics.org/knowledge-center/ethicsstat/.

[8] City of Birmingham Ret. & Relief Sys. v. Credit Suisse Grp. AG, No. 17 CIV. 10014 (LGS), 2019 WL 719751, at *6 (S.D.N.Y. Feb. 19, 2019).

[2] Having the Right Code

[a] Creating or Reviewing Your Code

[i] *Overview of Creating Your Code*

Regulators, prosecutors, courts and experts have all weighed in on the need for organizations to strengthen their efforts to promote ethics and integrity. Most have urged organizations to make a code of conduct the centerpiece of these efforts. Regulators have even provided settlements, mandates or just good guidance to illustrate what should be in this code. A variety of other resources are readily available to inform this process and provide advice and examples regarding the structure and substance of the code.

Organizational codes of conduct serve to set expectations and standards, provide information and guidance about those expectations and standards, and offer resources to help individuals understand and meet them. These goals will not be met by parroting requirements from the relevant regulator or borrowing a code from some other organization or expert. Instead, it will take careful consideration and appropriate answers to the questions below—answers that reflect a combination of regulatory mandates, industry issues, "best practices" and the unique culture and business of an organization.

[ii] *Who Will Draft or Review the Code?*

The first issue is who will be responsible for drafting or reviewing the code. Organizations often use legal or compliance staff for this purpose. These personnel are usually the best informed about both the general legal and regulatory requirements for the code and about the specific issues that must be addressed based upon the organization's business and regulatory environment. They can then vet the code draft with management, communications experts and other staff (such as line employees) to help ensure that the code is comprehensive, understandable and adequately addresses the concerns of supervisors and employees.

Some organizations have established drafting committees with representatives from legal, compliance, human resources, internal audit, corporate communications, marketing and key business units. The committee approach can make it easier to identify compliance-related issues and concerns from around the organization and make the code-drafting project a more high-profile and collaborative process, one that the business side of the organization has an investment in from the beginning. It can help ensure that the code is consistent in tone, style, and substance with other corporate policies and communications.

[iii] *What Kind of Code Should It Be?*

An important consideration is whether the code will be a high-level statement about the organization's mission, values and principles, or whether it will also include references to, and even details about, more specific policies and procedures. Is this a "code of ethics," a "code of conduct," or some of both? There can be a difference.

Codes of ethics, at least until the Sarbanes-Oxley Act, were generally expected to be shorter, focusing on fundamental corporate values such as fairness, honesty, and

integrity, and offering some guidance on how these values impact the daily activities of the organization and its employees. The Ethics Resource Center defines a code of ethics as

> [a] central guide and reference to assist day-to-day decision making. It is meant to clarify an organization's mission, values and principles, linking them with standards of professional conduct. As a reference, it can be used to clarify standards, organizational values and policies; promote effective decision-making; and direct users to identify relevant ethics-related resources within the organization.[9]

Organizations with "ethics" codes often include links or references to other source material for more specific policies and procedures.

By contrast, codes of *conduct* tend to include these ethics concepts while at the same time adding additional, more factual information about specific policies, compliance issues and acceptable (or unacceptable) actions regarding these issues. These codes are not legalistic; they should not read like the criminal law or a manual from a regulator, but they should state expected behaviors in the areas that they cover.

The Sarbanes-Oxley Act and related rulemaking from the SEC and the stock exchanges contain elements of both types of codes, mixing references to "honest and ethical conduct" with sections related to particular issues like conflicts of interest and the integrity of financial disclosures.[10] That is why a code combining ethics and values on the one hand with rules of conduct on the other may now make the most sense. After all, organizations choosing to have "aspirational" ethics codes will still have to find a way to address the more specific obligations under these rules.

No code can, or should, contain all of the policies and procedures in the organization. In some instances, such as with employment-related issues, the code can set forth basic rules about workplace conduct and security, while an employee handbook or human resources manual contains more technical and specific rules and procedures. Also, different business units or administrative areas will still need their own policies and procedures. This is particularly true in highly-regulated industries, where the link between legal and regulatory requirements and operational practices is most direct.

For example, the code can set forth the obligation of all employees to maintain accurate books and records, while the finance and accounting departments have their own policies and procedures to meet this obligation. The code of conduct for a publicly traded company should include the prohibition against insider trading and then refer to more detailed policies and procedures to help address this issue. Likewise, the code of conduct for a financial services company should make clear the duty of all officers, employees, directors and agents to treat customers fairly. More specific manuals and codes in a financial services organization will detail how investment advisors, financial professionals and other specialized staff must achieve this objective.

In another example, the Office of Inspector General of the federal Department of Health and Human Services ("OIG") recommends that organizations supplement their

---

[9] *See* Ethics & Compliance Initiative, Ethics and Compliance Glossary, *available at* https://www.ethics.org/resources/free-toolkit/toolkit-glossary/.

[10] *See, e.g.*, Sarbanes-Oxley Act § 406, 15 U.S.C.§ 7264.

"standards of conduct" with "a comprehensive set of written policies addressing all applicable statutes, rules and program instructions that apply to each function or department." These procedures for relevant legal and business risk areas should "articulate specific procedures personnel should follow when performing their duties."[11] In these cases, organizations often provide references or links in their general codes of conduct to the more specific and detailed policies.

[iv] *What Style Should Be Used?*

As with all issues around the drafting of the code, it is critical that the code reflect the organization's culture, management style and operations. The code must fit right in with the way the organization is run, and not stand apart as overly legalistic in an organization where policies and directives are generally short and straightforward, or overly simplistic in an organization that otherwise likes to spell out expectations and responsibilities in great detail.

The key is to remember the purpose of the code and its audience: this is not a legal brief for courts or regulators, but a means of communicating critical legal and compliance concepts to non-lawyers of varying levels of education and experience. The code is not a regulatory obligation; it represents an opportunity to reach and inspire employees. It is also the primary means of "selling" compliance and its importance to everyone connected with the organization. That is why the corporate communications and marketing departments can be valuable partners in marketing the code, as members of a drafting committee or otherwise in helping to review, distribute and publicize the code. Some companies have turned to groups of employees and executives—either informally or through focus groups—to test the clarity of the concepts and the relevance of the examples in their codes. Companies should not ignore their international employees in this vetting process.

[v] *Who Will Be Covered by the Code?*

Another question that companies must answer, after deciding what kind of code they want, is whether it will cover third parties such as agents, suppliers, contractors, consultants and distributors—in addition to—officers, directors, and employees. Will there be different codes for different groups of people depending on their title, location, function, or employment status?

To the extent that the values and rules in the code reflect the most important issues faced by the organization, the code can—and should—apply to the broadest range of individuals as possible. Both the NYSE and NASDAQ want the codes for their listed companies to apply at least to all directors, officers and employees. This has the advantages of consistency, clarity and a common set of expectations and norms from the top of the organization on down.

---

[11] *See* OIG's Compliance Program Guidance for Medicare+Choice Organizations Offering Coordinated Care Plans, 64 Fed. Reg. 61896 (Nov. 15, 1999) (explaining that the guidance "continues to be a major initiative by the OIG in its effort to engage the health care community in combating fraud and abuse"), *available at* https://oig.hhs.gov/fraud/docs/complianceguidance/111599.pdf. The OIG has issued similar compliance guidance plans for small-group physician practices (Oct. 5, 2000) and pharmaceutical manufacturers (May 5, 2003), reiterating the importance of internal controls in ensuring compliance.

Many companies go even further. For example, the Wal-Mart Statement of Ethics expressly applies to third parties:[12]

> Wal-Mart expects its suppliers, consultants, law firms, public relations firms, contractors and other service providers to act ethically and in a manner consistent with this Statement of Ethics. If you hire a service provider, you should take reasonable steps to ensure that the service provider has a reputation for integrity and ethical conduct and that the service provider is acting in a manner that reflects the highest ethical standards.

As discussed earlier in the chapter, the DOJ issued updated guidance on how prosecutors should evaluate corporate compliance programs in April 2019.[13] In determining whether the company has effectively integrated compliance into its daily operations, prosecutors are to consider whether the company has effectively communicated its policies to third parties.[14] Prosecutors should also "assess whether the company engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party."[15] This is a critical issue for organizations and their compliance programs. A company can delegate functions to these third parties, but it cannot delegate the legal and regulatory responsibility for how those functions are carried out. In addition, these third parties have the company's reputation and brand in their hands. Companies need to know who they are doing business with, and how that business is being conducted on their behalf.

Of course, if organizations are going to apply their codes to groups of non-employees—such as suppliers and vendors—they must make sure that those third parties know what is expected of them. A survey conducted in 2015 by Deloitte and Compliance Week found that 42% of responding chief compliance officers audited third-party compliance with company policies, while only 32% of respondents required third-party training and/or certification.[16] A continued increase of these percentages can further promote companies' compliance goals. In fact, according to research from The Risk Advisory Group, third-party risk was the number one priority for compliance professionals in 2018.[17]

[b] Structure of the Code

A number of important subjects are typically covered in codes of conduct, regardless of

---

[12] Wal-Mart Statement of Ethics at 2, *available at* http://media.corporate-ir.net/media_files/IROL/11/112761/corpgov/Ethics%20_Current.pdf.

[13] U.S. Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs, *available at* https://www.justice.gov/criminal-fraud/page/file/937501/download; *see also supra* § 13.02[1][i].

[14] U.S. Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs 4, *available at* https://www.justice.gov/criminal-fraud/page/file/937501/download.

[15] *Id.* at 7.

[16] *See* Deloitte, Third-Party Risks and Compliance Culture: CCOs' Top Challenges (Feb. 8, 2016), *available at* https://deloitte.wsj.com/riskandcompliance/2016/02/08/third-party-risks-and-compliance-culture-ccos-top-challenges-2/.

[17] *See* Compliance Horizon Report 2017: What is on the Compliance Horizon for 2018?, *available* at https://www.riskadvisory.com/campaigns/compliance-horizon-2017/.

which type and style are chosen in an organization. These include a leadership letter; purpose and goals; core mission and values; information about the compliance program and resources, including any reporting mechanisms; the protection of employees and agents against retaliation for reporting concerns; every individual's accountability for compliance; and the consequences of non-compliance.

[i] ***Statement from Leadership***

An introductory letter or statement from a senior executive (often the Chief Executive Officer) will explain the importance of ethics and compliance to the organization. This statement should articulate the personal, as well as institutional, commitment of senior management and the board of directors to ethical business practices and regulatory compliance. This sets the "tone at the top" and makes clear that ethics and compliance are part of the "culture" of the organization. The code, and the entire compliance program, will benefit from this emphasis. Not only is this stated commitment necessary for the rest of the employees to take these issues seriously, but regulators increasingly expect to see this kind of tangible demonstration by the leaders of the organization of their accountability and responsibility for compliance.

[ii] ***Purpose and Goals***

An introductory section should set forth the purpose and goals of the code of conduct and the overall compliance program, and also explain which populations within the organization are covered by the code. This section should emphasize the commitment of the organization—and the obligation of everyone connected with it—to comply with all applicable laws and regulations.

[iii] ***Mission and Values***

The organization's mission and values should be described in clear language. This section could include "ethical" values, such as integrity, respect, and fairness, together with "business-related" principles like commitment to customers, quality, and service excellence. It serves to put the code in the context of the organization's overriding principles and goals, and helps explain how compliance with the code will contribute to these goals. This section might even include practical examples of how to put these principles and values to work in meeting customers' needs or dealing with fellow employees.

[iv] ***The Compliance Program***

This section of your code should describe the compliance program, including the resources available to employees with questions or concerns about ethics and compliance issues, thereby demonstrating the organization's financial and staffing commitment to compliance and giving employees greater comfort about raising issues internally. The section typically includes references to the compliance officer and staff, any executive or board oversight committees and available training or other communications and materials about the program.

[v] ***Internal Reporting Mechanisms***

As part of the description of the compliance program, employees should be told about the means for requesting guidance or reporting concerns. Codes may suggest that

employees consult with supervisors or internal resources such as human resources or the legal or compliance staff. In addition, it is becoming increasingly common for organizations to maintain 1-800 numbers—called compliance "hotlines" or "helplines"—for employees to use if they are uncomfortable raising issues in these other ways, or if they are unsatisfied with the response they receive regarding their concerns. The phone lines, which may be answered by compliance staff or by external vendors, also serve as an anonymous reporting mechanism, giving organizations a means of complying with Section 301 of the Sarbanes-Oxley Act, regarding "confidential, anonymous" complaints to the audit committee about financial and accounting matters.[18]

Companies may also provide dedicated email addresses, web-based reporting tools or mail drops for these communications and make these mechanisms available to customers and other external stakeholders in addition to employees. It is advisable to provide employees with multiple means of raising compliance questions or concerns—by hotline, dedicated email, letter or phone call—to encourage as many employees as possible to come forward and ask for help or make reports. Communications about these reporting tools should make clear that employees have the right to report matters anonymously and confidentially, to the extent that the needs of the investigation and possible cooperation with external authorities will allow identities to be protected. Many companies include in this section of the code a requirement that employees report any possible misconduct.

Organizations should record and track all communications through these vehicles, and establish procedures to investigate the matters and report the results of these investigations back to the individuals who initiated the communications. Everyone who is likely to receive a report of possible misconduct—including supervisors—should be trained on the appropriate response and follow-up. The organization must also ensure that appropriate procedures are in place, and enforced, to escalate reports.[19]

[vi] *Non-Retaliation*

Every code of conduct must include a statement of the organization's policy protecting employees against retaliation or retribution for reports about compliance matters. This is critical to ensure that whistleblowers are protected in accordance with the Sarbanes-Oxley Act, the Dodd-Frank Act and other requirements. It is also in the organization's best interest to encourage employees to report these issues internally so that the organization has the first opportunity to evaluate and address them. According to research from the Ethics Resource Center, one of the most common reasons why employees do not report misconduct is fear of retaliation. This fear not only increases the chances of external reporting and of a separate claim of mistreatment of the employee; it deprives the organization of the information needed to stop problems from growing. This same research shows that retaliation rates steadily and substantially

---

[18] *See* 15 U.S.C. § 78j-1(m)(4)(B).

[19] *See, e.g.*, Deloitte, Boards: Understand the Rules for Ethics and Compliance Oversight—Audit Committee Resource Guide (2018), *available at* https://deloitte.wsj.com/riskandcompliance/2018/05/02/boards-understand-the-rules-for-ethics-and-compliance-oversight/.

decline in organizations with comprehensive ethics and compliance programs and when managers across the organization encourage rather than discourage reports.[20] When the ethical culture is weak, companies suffer more misconduct and more retaliation.

Moreover, a decision by the United States Supreme Court has broadened the category of employment actions that can constitute prohibited retaliation—at least in the employment discrimination context—placing an additional premium on organizational efforts to prevent and identify any conduct that could be considered retaliatory.[21] As discussed earlier in the chapter, however, the Supreme Court has recently narrowed the types of reports that qualify for whistleblower protection under Dodd-Frank—protecting only applicable complaints made to the SEC, not purely internal reports.[22]

[vii] *Personal Responsibility and Certification*

The code provides an opportunity to make clear the personal responsibility of directors, officers, supervisors and employees for complying with the code and related standards of conduct. Organizations are increasingly including compliance factors—and ethics and integrity—in their performance evaluations, decisions on compensation and promotion and other employment-related decisions. If so, that should be mentioned in the code.

Companies now often insist that employees sign a certification or pledge, at the end of the code or as part of code-related training, indicating that they have read the code and intend to comply with it. This certification is generally done annually. A "typical" certification states:

> I have read and understand the provisions of the [] Corporation code of conduct. I will abide by the standards of conduct contained in the code and in company policies. I will complete all required training courses on ethics and compliance topics including training on the code. I will speak up, using the resources listed in the code, if I am in doubt as to the proper course of conduct or if I become aware of possible violations of our standards or the law.[23]

In some cases, this certification may also indicate that the employee has reported to the compliance office any known violations of the code of conduct or other relevant company policies.

[viii] *Consequences of Non-Compliance*

Together with personal responsibility, the code should explain the consequences of non-compliance. This discussion may include a summary of the organization's

---

[20] *See* Retaliation: When Whistleblowers Become Victims, A Supplemental Report of the 2011 National Business Ethics Survey, *available at* http://jpp.whs.mil/Public/docs/03_Topic-Areas/06-Retaliation/20150410/06_ERC_RetaliationWhenWhistleblowersBecomeVictims.pdf.

[21] *Burlington Northern & Santa Fe Railway Co. v. White*, 548 U.S. 53 (2006); *see also* Thompson v. N. Am. Stainless, LP, 562 U.S. 170, 173–74 (2011) (reaffirming that the anti-retaliation provision of Title VII covers a "broad range of employer conduct").

[22] *See supra* § 13.02[2][b][ii] (discussing *Digital Realty Trust, Inc. v. Somers*, 138 S. Ct. 767 (2018)).

[23] Navex Global, Annual Code Acknowledgements, *available at* https://www.navexglobal.com/en-us/resources/datasheets/annual-code-acknowledgements?RCAssetNumber=150.

processes for investigating and disciplining compliance violations, and any other means by which everyone, throughout the organization, will be held accountable for compliance performance.

[c] Subjects in the Code

Organizations that choose to include business conduct issues in their codes, in addition to ethics and values, must next decide what subjects to cover, in addition to the sections we have just reviewed. This requires an analysis of more than just the regulations of the SEC and the stock exchanges; it also requires an assessment of each organization's specific legal and regulatory risks and issues. The assessment should reflect the nature and size of the business; industry regulations and concerns; the jurisdictions in which the organization does business, including any countries outside the United States; and any recent internal audits, investigations, regulatory actions or lawsuits.

The Ethics & Compliance Toolkit from the Ethics Resource Center has a comparable list of "common provisions found in organizational codes." In addition to topics already discussed, these include anti-bribery; accuracy of books and records; conflicts of interest; political activity; confidentiality and disclosure of inside information; employment practices (*e.g.*, workplace relationships and conduct); environmental compliance; health and safety; internet and social media; and relationships with third parties.[24]

[3] Successfully Implementing the Code

[a] The Overall Compliance Program

As we have seen throughout this chapter, the code of conduct must be placed in the context of the overall compliance program that organizations are increasingly expected to implement. The code may well be the foundation of this program, but it will not achieve its objectives without the other elements to make it known, understood, used, monitored, enforced, and improved when necessary. In each of the compliance-related recommendations and mandates that we have reviewed, the code of conduct is expected to be reinforced by mechanisms to take it off the shelf and make it work throughout the organization.

Before closing, we briefly discuss some of the other elements that should be included in an organization's compliance program to ensure that the code will have the necessary infrastructure and support to achieve its objectives. These programs are an effective combination of process and substance: process to incorporate the elements of the FSGO and provide the tools needed to impact behavior; and substance to address the substantive legal and compliance issues that are most important to the organization.

[b] Status and Resources—The Tone from the Top

[i] *The Tone from the Top*

Nothing is more critical to the success of a compliance program—and more essential to the creation of a compliance culture—than active and constant support from the top.

---

[24] *See* Ethics & Compliance Toolkit, Common Code Provisions, *available at* https://www.ethics.org/resources/free-toolkit/code-provisions/.

As noted by Richard G. Ketchum, then-Chairman and CEO of the Financial Industry Regulatory Agency (FINRA), "[t]he board, the CEO, business leaders and the CCO all play critical roles in setting the tone at the top and establishing an organization's values and ethical climate. The tone carries through to every aspect of the organization's structures, policies, processes and training."[25]

It takes time and resources to write an effective code of conduct for an organization, and far more time and resources to make the code come alive in that organization. Companies that are serious about compliance must be willing to commit the resources to make this happen. Organizations must give their compliance programs sufficient status and stature to persuade officers and employees to take the program seriously. One way to accomplish both objectives is for the board of directors to formally adopt the compliance program, including the code of conduct, thus signifying its importance to senior management and the entire organization.

Another way is to set and communicate the right tone from the top, as demonstrated by the answers to the following questions.

[ii] *Who Owns Compliance?*

One key to an effective compliance program is clarity regarding the ownership of compliance and about the right division of responsibility for compliance-related activities. The Compliance staff cannot be the sole owners of the organization's legal and regulatory obligations. Instead, the Compliance Department should be responsible for the "pre" and "post" of compliance:

> "Pre": This means helping supervisors and employees identify, understand and address the significant legal and regulatory requirements associated with their part of the business. The code of conduct is the central element in meeting this responsibility.
>
> "Post": Compliance should organize efforts to check, from time to time, on how well business units and employees are doing at meeting these requirements.

It is critical that business leaders and their employees are held responsible for what comes in between: actual compliance with these requirements. Senior leadership must make this clear throughout the organization. One way that regulators will judge the sincerity of a company's commitment to compliance is by assessing if compliance is a business function—not just something the company has to do but something it wants to do and insists that its business executives own.

[iii] *Who Is the Compliance Officer?*

Organizations should have a compliance officer who can command attention throughout the organization and must give that compliance officer direct and regular access to senior management and to the board of directors. As the SEC has explained, the compliance or ethics officer identified in an organization's code of conduct must have "sufficient status within the company to engender respect for the code and the

---

[25] Richard G. Ketchum, FINRA Chairman and Chief Executive Officer, Remarks From the 2016 FINRA Annual Conference (May 23, 2016), *available at* https://www.finra.org/newsroom/speeches/052316-remarks-2016-finra-annual-conference.

authority to adequately deal with the persons subject to the code regardless of their stature in the company."[26] Similarly, the DOJ's April 2019 Evaluation Memorandum instructs prosecutors to consider "whether those responsible for compliance have: (1) sufficient seniority within the organization; (2) sufficient resources, namely, staff to effectively undertake the requisite auditing, documentation, and analysis; and (3) sufficient autonomy from management, such as direct access to the board of directors of the board's audit committee." As the Evaluation Memorandum recognizes, however, the "sufficiency of each factor . . . will depend on the size, structure and risk profile of the particular company" at issue.[27]

Compliance officers often report directly to the CEO or to some other high-level executive such as the general counsel. Some also have a "dotted line" to the audit committee of the board of directors, reflecting their ability to report directly to the board in the event of serious compliance violations or allegations of misconduct by senior executives. In these cases, according to the Ad Hoc Advisory Group, compliance officers must be able to report to the organization's governing authority "without the potential filtering or censuring influence of senior organization managers."[28] The DOJ's Evaluation Memorandum also recommends that prosecutors should consider whether compliance officers and representatives of other relevant control functions "have direct reporting lines to anyone on the board of directors and/or audit committee," how often the compliance officers "meet with directors," and whether "members of [] senior management [are] present for these meetings."[29]

The definition of an "effective" compliance program in the FSGO includes that "[i]ndividual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effective-ness of the compliance and ethics program." A direct reporting line to the board or a sub-group (such as the Audit Committee) is also

---

[26] *See* SEC Release No. 33-8177, Disclosure Required by Sections 406 and 407 of the Sarbanes-Oxley Act of 2002 at n. 45 (Jan. 23, 2003), *available at* https://www.sec.gov/rules/final/33-8177a.htm.

[27] *See* U.S. Dep't of Just., Criminal Division, Fraud Section, Evaluation of Corporate Compliance Programs (April 30, 2019), *available at* https://www.justice.gov/criminal-fraud/page/file/937501/download; *see also* USSG § 8B2.1(b)(2)(C), *available at* https://www.ussc.gov/guidelines/2018-guidelines-manual/2018-chapter-8 ("[The compliance officer] shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.").

[28] Report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines at 62 (Oct. 7, 2003), *available at* https://www.ussc.gov/sites/default/files/pdf/training/organizational-guidelines/advgrprpt/AG_FINAL.pdf.

[29] *See* U.S. Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs, *available at* https://www.justice.gov/criminal-fraud/page/file/937501/download. *See also* Rand Corporation, Transforming Compliance: Emerging Paradigms for Boards, Management, Compliance Officers, and Government (May 28, 2014), *available at* https://www.rand.org/pubs/conf_proceedings/CF322.html (emphasizing that a "key ingredient for an 'effective' ethics and compliance program is an independent and empowered CCO").

required for credit for an effective compliance program under the FSGO in certain circumstances.[30]

These guidelines have energized the debate about whether the compliance officer must report to the CEO or the board, with some in the compliance community arguing that the chief compliance officer *must* be a separate, highest-level corporate officer who reports directly to the CEO, rather than to the general counsel, for example. They assert that, "[p]rograms led by an individual reporting to either the CEO or the board . . . substantially outperform those reporting to the general counsel;" giving "a more prominent 'seat at the table' for chief compliance officers reflects the greater importance accorded to their role and the issues in their organizations."[31]

As discussed earlier in the chapter, regardless of how a company chooses to structure the compliance officer's reporting, senior management may be held responsible for the effectiveness of the compliance program. In a 2018 action taken by the SEC against a company's chief compliance officer for failing to establish and maintain a reasonable supervisory system, the SEC emphasized that the CCO was "not the only person" at the company responsible for the deficiency, and claimed that the CEO "abdicated his own responsibilities" in failing to ensure the CCO's effectiveness.[32] Likewise, the SEC adjusted the reporting relationship of its own internal ethics office—from the general counsel to the chairman—in response to a critical report by its Office of the Inspector General.[33]

DOJ enforcement actions have also, to some extent, entered this debate. In a deferred prosecution agreement with HSBC, filed in December 2012 to settle charges that the bank failed to meet its obligations to prevent money laundering, the bank agreed to separate its legal and compliance functions and make the chief compliance officer one of its 50 senior-most leaders.[34] However, the DOJ has not insisted in all cases that the chief compliance officer report directly to the board or to the CEO, or be a separate executive officer from the general counsel. An analysis reported by the Society for

---

[30] *See* USSG §§ 8B2.1(b)(2)(C), 8C2.5(f)(3)(C)(i), *available at* https://www.ussc.gov/guidelines/2018-guidelines-manual/2018-chapter-8.

[31] *See* LRN, The 2014 Ethics and Compliance Program Effectiveness Report, *available at* https://content.lrn.com/research-insights/2014-e-c-program-effectiveness-report.

[32] *See In the Matter of the Application of Thaddeus J. North For Review of Disciplinary Action Taken by FINRA,* Exchange Act Release No. 84500 (Oct. 29, 2018), *available at* https://www.sec.gov/litigation/opinions/2018/34-84500.pdf.

[33] *See* Statement from Chairman Schapiro on IG Investigation, 2011-187 (Sept. 20, 2011) and linked Report of Investigation (at p. 117), *available at* http://www.sec.gov/news/press/2011/2011-187.htm. Note, however, that the report and recommendations of the SEC Inspector General were in response to an alleged impropriety involving the SEC's general counsel.

[34] *See* U.S. v. HSBC Bank, Cr. No. 12-763, (E.D.N.Y. Dec. 11, 2012). *See also* U.S. Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs, *available at* https://www.justice.gov/criminal-fraud/page/file/937501/download (instructing prosecutors to consider how the "compliance function compare[s] with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers" in evaluating corporate compliance programs).

Corporate Compliance and Ethics ("SCCE") of 31 deferred prosecution and non-prosecution agreements executed between 2007 and 2010 found that 23 provided specific guidance on the reporting line for the chief compliance officer. Twenty-one required that the compliance officer have the authority to report matters directly to the board, while only seven required that the compliance officer be directly supervised by the company's CEO.

More important than the reporting relationship are the chief compliance officer's competence and the support and integrity of the senior leadership of the organization. As explained by then-SEC Commissioner Luis Aguilar, "[t]he need for senior leadership to support CCOs is not just good practice, but also a business necessity."[35] Commissioner Aguilar cited an SEC enforcement case where the Commission took disciplinary actions against a firm President for failing to adequately support the firm's CCO, despite the CCO's repeated requests for additional support.[36]

In March 2017, the Health Care Compliance Association and OIG issued a guide for compliance program effectiveness, recommending that boards review and approve their companies' compliance plans annually. In particular, boards should verify that appropriate compliance policies and procedures exist and "assure [that] governance policies related to compliance are appropriately maintained."[37] It should finally be noted in this regard that, as the "profession" of compliance officer has developed, various organizations have begun to create Standards of Conduct for the role and even to devise certification training and tests.[38]

[iv] *What Are the Resources for Compliance?*

The compliance officer must have the commitment of resources to effectively implement the code of conduct, regardless of where he or she sits on the organization chart. The DOJ advises that prosecutors begin their evaluation of a company's compliance program by determining "the degree to which the program devotes appropriate . . . resources to the spectrum of risks."[39] Prosecutors should consider whether compliance programs have been adequately staffed, whether sufficient funds

---

[35] Luis A. Aguilar, SEC Commissioner, The Role of Chief Compliance Officers Must be Supported (June 29, 2015), *available at* https://www.sec.gov/news/statement/supporting-role-of-chief-compliance-officers.html.

[36] *Id. (citing In the Matter of Pekin Singer Strauss Asset Management Inc., Ronald L. Strauss, William A. Pekin, and Joshua D. Strauss*, Advisers Act Rels. No. 4126 (June 23, 2015), *available at* http://www.sec.gov/litigation/admin/2015/ia-4126.pdf).

[37] HCCA-OIG Compliance Effectiveness Roundtable, Measuring Compliance Program Effectiveness: A Resource Guide (Mar. 27, 2017), *available at* https://oig.hhs.gov/compliance/compliance-resource-portal/files/HCCA-OIG-Resource-Guide.pdf.

[38] *See, e.g.*, Ethics and Compliance Initiative, "High Quality Program Assessment," *available at* https://www.ethics.org/high-quality-compliance-program-assessment/; Society of Corporate Compliance and Ethics, "Become Certified," *available at* https://www.corporatecompliance.org/certifications/become-certified.

[39] U.S. Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs, *available at* https://www.justice.gov/criminal-fraud/page/file/937501/download.

have been allocated to compliance teams, and whether the company grants compliance requests for additional resources, such that compliance personnel can "effectively audit, document, analyze, and act on the results of the compliance efforts."[40]

Senior management and boards of directors must ask themselves the kinds of questions about their compliance programs that regulators and prosecutors will ask: have they provided that the people and other resources—either within the compliance department or from other departments within the organization—will:

- conduct compliance training and otherwise communicate compliance standards and expectations;
- analyze and respond to hotline calls;
- regularly track and evaluate new laws and regulations;
- monitor and audit business unit compliance performance;
- report to directors and senior management on compliance performance; and
- respond firmly and effectively to issues, problems and violations.

These resources need not all be within a centralized compliance function. A growing number of organizations—especially those with large numbers of employees and locations around the world—have adopted a "hybrid" approach in which the corporate compliance staff is augmented by resources "on-the-ground" in various business units or international markets. The localized resources can be full-time or part-time. They offer colleagues accessible, business-knowledgeable assistance and can be linked to the organizational compliance objectives through their compliance with standards set up by the corporate compliance leaders, and by periodic reporting to headquarters and participation on a company-wide compliance committee.

For example, when the multinational drug maker Eli Lilly & Co. settled shareholder lawsuits in 2010 regarding the improper marketing of drugs, it agreed to create four new senior-level compliance positions, all reporting to its chief ethics and compliance officer: a vice president for global compliance strategy and risk management; a compliance business liaison to work with U.S. and international affiliates; a senior director of enterprise risk management; and a compliance project manager.

Similarly, in July 2019, social media company Facebook entered into a settlement with the Federal Trade Commission ("FTC") to resolve charges that the company violated a 2012 FTC order by misleading users about their ability to control the privacy of their personal information. As a part of the settlement, Facebook is required to create a new independent privacy committee of its Board of Directors to monitor the protection of user data and designate compliance officers in the organization to oversee the privacy program.[41]

---

[40] *Id.*

[41] *See* FTC Press Release, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook" (July 24, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions; Mike Isaac and Natasha Singer, "Facebook Agrees to Extensive New Oversight as Part of $5 Billion Settlement," N.Y. Times (July 24, 2019),

[v] *How Is Senior Leadership Involved with the Compliance Program?*

Many organizations have established internal compliance and ethics committees to help organize, strengthen and promote compliance efforts even after the code has been drafted and implemented. These committees may include senior-level representatives of internal audit, legal, human resources, information technology, corporate security and line business units, in addition to compliance officers. These committees communicate the organization's commitment to compliance and the importance of the practical, business application of ethics and integrity to the most senior executives.

Besides sending the message about the importance of compliance, these compliance leadership teams may also:

- identify and track the organization's response to new legal and regulatory requirements;
- oversee the company's compliance risk assessment and match compliance resources and actions to those risks;
- develop and oversee the implementation of an annual compliance plan;
- set standards for compliance activities in the business units;
- develop tools for communicating, training, monitoring and reporting about compliance; and
- ensure the application of appropriate compliance controls to new business initiatives.

Another good way to ensure that senior executives "lead" compliance and ethics is through the compensation system. In this connection, companies may include ethics as a component of a manager's performance evaluation, which is used in connection with the annual or other periodic compensation review. For example, a report by the Society of Corporate Compliance and Ethics lists the following factors that executives should consider in employee evaluations:

- Does the manager use "the code of conduct and encourage[] subordinates to do the same"?
- Does the manager "[a]ctively take[] steps to implement the compliance program and the code of conduct"?
- Does the manager "[a]ttend[] appropriate compliance training, and make[] sure subordinates get appropriate training and know the rules that apply for their jobs"?
- Is the manager "willing to challenge questionable conduct or proposals"?[42]

Senior leaders further demonstrate their commitment to compliance when they are willing to discipline high-ranking and successful employees for compliance violations—

---

available at https://www.nytimes.com/2019/07/24/technology/ftc-facebook-privacy-data.html.

[42] *See* Joseph E. Murphy, "Using Incentives in Your Compliance and Ethics Program" (Nov. 2011), *available at* https://assets.hcca-info.org/Portals/0/PDFs/Resources/library/814_0_IncentivesCEProgram-Murphy.pdf.

and terminate their employment when warranted—and when they walk away from business if the compliance risks are too great. In a 2017 action involving Linde North America Inc., for example, the DOJ declined to prosecute the company for FCPA violations, acknowledging that Linde fired and/or disciplined high-level executives involved in the misconduct and terminated existing contracts with the offending management company.[43]

[vi] ***Enterprise Risk Management***

One trend that has accelerated in recent years is to consider the compliance function as part of a consolidated Enterprise Risk Management ("ERM") team. Under this approach, compliance is combined with Internal Audit, the Sarbanes-Oxley oversight staff and often a "strategic risk management" team under the leadership of a senior executive, more typically as part of finance rather than legal. The ERM approach accomplishes at least three objectives for organizational compliance. First, it gives the compliance team ready access to the internal audit resources and business process oversight needed to accomplish compliance objectives. Second, it places the compliance program squarely in the context of the organization's overall approach to risk, thus making more obvious the contributions that compliance is making to business objectives. Third, this ERM process is most often driven by the organization's CEO and board of directors.

The need for effective risk management has taken on new urgency since the financial crisis at the end of the previous decade. One consequence is that companies, regardless of industry, are now being evaluated on the capabilities and effectiveness of their risk management efforts. Standard & Poor's, for example, now includes ERM reviews when meeting with management to review a company's credit rating. In assessing risk management culture, or "the importance accorded to risk and ERM in all key aspects of . . . business operation and corporate decision-making," S&P focuses on a firm's "risk appetite framework, risk governance and organizational structure, risk communications and reporting, and the embedding of risk metrics in its compensation structure," as well as "the degree to which there is broad understanding and participation in risk management throughout the organization."[44] Financial services and insurance companies face even more in-depth reviews of their ERM including their culture of compliance and ethics.

In a 2011 speech at the National Society of Compliance Professionals National Meeting, Carlo di Florio, then-Director of the SEC Office of Compliance Inspections and Examinations, emphasized "the heightened role of ethics in an effective regulatory compliance program, and the role of both ethics and compliance in enterprise risk

---

[43] *See* Letter from Laura N. Perkins, Assistant Chief, Fraud Section U.S. Dep't of Justice to Lucinda Low and Thomas Best, Counsel to Linde North America Inc. (June 16, 2017), *available at* https://www.justice.gov/criminal-fraud/file/974516/download.

[44] *See* Standard & Poor's Rating Services, Enterprise Risk Management (Mar. 28, 2014), *available at* https://www.spratings.com/scenario-builder-portlet/pdfs/ICSB_Enterprise_Risk_Management.pdf.

management."[45] He stressed that stakeholders increasingly expect firms to meet heightened standards for ethical behavior, and that the SEC examination program would place a greater emphasis on risk assessment by "meeting boards of directors, CEOs and senior management to share perspectives on the key risks facing the firm, how those risks are being managed and the effectiveness of key risk management, compliance, ethics and control functions."[46]

[c] Communications and Training

The adoption of a new or revised code of conduct should be a significant event, one that is accompanied by a comprehensive communications and training program to emphasize the importance and value of the code, and raise its profile, within the organization. To drive the right behaviors throughout the business and workforce, an organization needs a comprehensive communications plan that emphasizes the importance of compliance. This plan should have three parts: (1) raising awareness about the importance of compliance issues; (2) engaging leaders and employees at all levels of the organization in conversations about compliance and ethics through meetings, town halls, focus groups and one-on-ones; and (3) driving behavior—using the results of these interactions to make the compliance program and tools more relevant and effective.

The awareness campaign can begin with the distribution of the code of conduct to all identified stakeholders, in addition to any public disclosures mandated by the regulators, and this distribution can be accompanied by a wide variety of internal communications and compliance-related events to raise awareness and interest.

Organizations may distribute compliance bulletins, newsletters, regular e-mails or special reports on the code and any new regulations or recent enforcement actions. Some have created in-house compliance videos or instituted compliance awards ceremonies to recognize employees and business units for their compliance performance and commitment. Others have posters, payroll inserts, wallet cards or telephone stickers with the compliance hotline number. Organizations may also have compliance sites on their internal websites for employees to read the code and related policies and procedures, access other resources and take on-line training courses.

Companies are increasingly providing training to all employees and others who are covered by their codes, and are also providing introductory compliance training to new employees. Organizational training plans often include both in-person training and on-line training with the subject matter falling into two categories: general compliance awareness and code of conduct training, on the one hand, and training about more specific compliance risks related to particular jobs, on the other. This compliance communications and training program cannot be static and, if at all possible, it should not stay at headquarters. As cost-effective as on-line training can be, companies should

---

[45] Carlo V. di Florio, Director SEC Office of Compliance Inspections and Examinations, The Role of Compliance and Ethics in Risk Management (Oct. 17, 2011), *available at* https://www.sec.gov/news/speech/2011/spch101711cvd.htm.

[46] *Id.*

consider in-person training at those business units and geographic areas where compliance risks are highest and the likelihood of mistakes or misunderstandings the greatest.

Moreover, compliance training cannot be "once and done"—a one-time event that accompanies the launch of a new code or the settlement of a compliance matter, and then does not occur again until the next investigation. Compliance training must be part of the regular rhythms and activities of the organization.

Organizations operating outside the United States need to consider translating the code and compliance training into other languages, and whether some of the provisions and examples in the code need to be modified to reflect local practices, issues and concerns. These organizations also need to provide access to any reporting mechanisms, such as hotlines, for employees and others outside the United States, to the extent permitted by local data privacy and labor laws.

[d] Monitoring and Auditing

It has been said that organizations manage what they measure. If compliance with the code of conduct is important to an organization, then the roll-out of the code should be accompanied by a comprehensive plan to measure and monitor the compliance performance of the business units and individuals subject to the code. This can include regular reporting of compliance performance indicators as well as periodic audits of particular issues, conducted by internal audit or compliance staff.

In this regard, organizations need to determine what these performance indicators will be and how they can be identified, measured and reported. To be most effective, these efforts should be consistent with how the business is managed in general. There should be two categories of indicators, one for the compliance staff and one for the business. This will reinforce the essential point that compliance is every business unit's—and every individual's—responsibility, not just the job of the compliance team.

The first set of indicators reflects the activities of the *compliance* department and staff such as: the number and types of training programs conducted; any communications released to staff; the number and results of compliance-related audits; the number, type and outcomes of calls to the compliance hotline; any regulatory examinations, investigations, audits or inquiries that were handled by compliance; and any compliance-related customer complaints.

The other category of indicators reflects the compliance-related performance of *business* units. These indicators will generally be industry-specific. In health-insurance organizations, for example, they could include reports on the timeliness of claims processing, the handling of requests for service, the licensing of sales staff and the volume and substance of customer complaints. In financial services, compliance performance indicators could include measures of sales practices such as suitability of sales agent disciplinary actions, investigations or inquiries by regulators, agent and client retention, timeliness and frequency of customer transactions, monitoring of employee stock trades and field audit results. Each business unit should create a

compliance plan that incorporates these key indicators, required remediation from internal audits, responses to regulatory matters and other commitments to regulators and external stakeholders.

Both categories of compliance performance indicators should relate to the most important regulations impacting the organization and be reported regularly to senior business management and to the board of directors.

The compliance program guidance from the OIG puts it this way:

> [A]n effective program should incorporate thorough monitoring of its implementation and an ongoing evaluation process. The compliance officer should document this ongoing monitoring, including reports of suspected noncompliance, and share these assessments with . . . senior management and the compliance committee.[47]

The OIG adds that "one effective tool is the performance of regular, periodic compliance audits by internal or external evaluators who have expertise in Federal and State health care statutes, regulations, and program requirements, as well as private payor rules."

The Association of Healthcare Internal Auditors developed the following "Seven-Component Framework" for compliance auditing and monitoring: "perform a risk assessment and determine the level of risk[;] understand laws and regulations[;] obtain and/or establish policies for specific issues and areas[;] educate on the policies and procedures and communicate awareness[;] monitor compliance with laws, regulations, and policies[;] audit the highest risk areas[;] re-educate staff on regulations and issues identified in the audit."[48]

Regardless of the compliance performance indicators or monitoring and auditing techniques that are used, organizations must have a structured means of responding to identified issues and documenting these responses. Some organizations have developed special tracking reports—or use existing management and performance reports—to ensure that identified compliance-related deficiencies are properly and timely remediated.

[e] Logging, Investigating and Reporting

Regulators also expect organizations to implement effective processes for investigating all of the compliance-related matters that are reported through the various tools described earlier in the chapter. This enables companies to prevent problems in the first instance, keep small issues from becoming big problems, identify trends or other potential company-wide concerns and—in each instance—investigate and effectively address compliance concerns without outside intervention. Such processes also help

---

[47] *See* OIG Compliance Program Guidance for Nursing Facilities, 64 Fed. Reg. 14289, 14302 (Mar. 16, 2000), *available at* https://oig.hhs.gov/authorities/docs/cpgnf.pdf. The OIG reiterated this guidance when it issued its most recent compliance guidance report in September 2008. *See* OIG Compliance Guidance, *available at* https://oig.hhs.gov/compliance/compliance-guidance/index.asp.

[48] Mark P. Ruppert, "Defining the Meaning of 'Auditing' and 'Monitoring' & Clarifying the Appropriate Use of the Terms," *available at* https://ahia.org/assets/Uploads/pdfUpload/WhitePapers/DefiningAuditingAndMonitoring.pdf.

encourage employees to feel comfortable reporting internally, and demonstrate the organization's responsiveness and commitment to compliance in the event of external scrutiny.

[f] Annual Compliance Plan

Some organizations have annual compliance plans, just as they have annual business plans. These plans typically reflect the regulations applicable to the business, industry practices and issues, the size and structure of the organization and its compliance history, and include elements for members of the business to complete—not only for members of compliance.

The level of effort and resources committed to the compliance planning process is a tangible reflection of the priority attached to the program by the leadership of the organization. The planning process may also serve as a helpful measure of whether the compliance staff is knowledgeable of what is going on throughout the business and can effectively influence organizational and individual behavior.

[g] Review and Modification

The compliance program should also have a built-in process for reviewing and modifying the code, and the other elements of the program, in response to changes in business conditions, new laws and regulations or problems that have been identified.

Peter Driscoll, Director of the SEC's Office of Compliance Inspections and Examinations, has emphasized the importance of "annual compliance program reviews" that "address the adequacy of the adviser's policies and procedures." He stated:

> Internal policies, procedures, and controls are the first line of defense against adviser misconduct and must be tailored to the adviser's business and followed . . . . [We] encourage[] advisers to reflect upon their own practices, policies and procedures in these areas and to improve their compliance programs.[49]

Some organizations have a formal process for identifying, communicating and tracking compliance with the laws and regulations. These organizations designate business and legal "issue owners" for the various categories of laws and regulations that apply to the business, and then assure that appropriate processes and resources are in place to identify and address changes in laws and regulations in these areas. This has the added advantage of helping integrate and embed compliance issues and concerns into business units throughout the organization. Another approach to this process is for the compliance and legal staffs to identify and evaluate each new law and regulation, send a description to each business unit that might be impacted and require the business units to explain how they will comply. The compliance department will then periodically check with the business units to determine if they are in full compliance.

---

[49] Peter B. Driscoll, then-Acting Director of the SEC Office of Compliance Inspections and Examinations, Improving Investment Adviser Compliance (Sep. 14, 2017), *available at* https://www.sec.gov/news/speech/speech-driscoll-2017-09-14 (also identifying various issues with policies and procedures that "provide[] employees with only general guidance, identif[y] limited examples of safeguards for employees to consider, [are] very narrowly scoped, or [are] vague and d[o] not articulate procedures for implementing the policies").

This allows the organization to adjust its compliance program based on any new regulatory mandates that are identified and to track and document its efforts. Another useful technique is to formally include compliance as an express part of each new business initiative. As one SEC official stated:

> Business models, rules, ethical standards and compliance tools are continually evolving. Yet, recent studies show that compliance officers may not be focusing on emerging risk areas . . . . Leading organizations ensure that they stay in front of these changes through a process of ongoing improvement that leverages new technology and best practices.[50]

[h] Employee Surveys of the Company's Compliance Culture

In addition to using the compliance performance measures described above, some organizations use employee surveys to assess employee attitudes about the compliance culture and program. These surveys can measure employee attitudes about the "tone at the top," awareness about the compliance program elements, willingness to ask for help and raise issues without fear of retaliation and perceptions about their managers' commitment to doing the right thing. According to the Ethics and Compliance Initiative, "in organizations where employees perceive that [a high-quality ethics and compliance program] element is present, favorable ethics program outcomes are increased more than 10 [times]."[51] Indeed, this attitude about the organization's "institutional justice" is a prime determinant of an employee's willingness to report misconduct internally.[52] Organizations that are willing to test and address these attitudes on the front lines will be better able to create, promote, maintain and demonstrate the kind of culture of ethics and compliance that regulators, prosecutors and compliance experts increasingly expect.

[4] Four Substantive Principles to Guide the Compliance Program

Here are four substantive principles to keep in mind in drafting and revising the code of conduct, and in reviewing and enhancing the organization's compliance program.

(1) Good business equals good compliance. Processes and tools—including relevant, understandable policies and procedures—that improve the effectiveness of business operations will also promote compliance and integrity.

(2) There should be no gap between the size and complexity of the business and the scope of its code of conduct and overall compliance program. Compliance policies, controls and tools must reflect the specifics of—and changes in—the business, and must be built into and alongside new business initiatives and

---

[50] Stephen L. Cohen, SEC Associate Director of Enforcement, Remarks at SCCE's Annual Compliance & Ethics Institute (Oct. 7, 2013), *available at* https://www.sec.gov/news/speech/spch100713slc.

[51] Ethics & Compliance Initiative, Global Business Ethics Survey: Measuring the Impact of Ethics & Compliance Programs 6 (June 2018), *available at* https://acua.org/ACUA/media/files_members/rise/webinars/Measuring-the-Impact-of-Ethics-and-Compliance-Programs-June-2018.pdf.

[52] *Id.* at 6, n.2 (identifying that "[e]mployees in stronger cultures [] were more likely to report misconduct compared with those in weaker cultures" and that "[w]hen employees felt encouraged to speak up[,] even with bad news, favorable ethics outcomes increased by 14 [times]").

technologies.

(3) Companies' compliance endeavors will be held to standards of "best practices" and compared to what other companies are doing in their own compliance programs. As reflected earlier in this chapter, regulators are becoming more demanding about what good compliance programs and cultures should look like, and they will judge companies' compliance programs according to increasingly high standards.

(4) Keep in mind the two goals of organizational compliance: to prevent, detect and respond appropriately to any violations of laws, regulations and company policies; and to limit organizational responsibility for the inevitable violations by individuals, because of everything the company did to meet the first goal before those violations occurred.

§ 13.04 Conclusion: The Importance of the Compliance Program

Compliance and ethics programs do make a difference, as judged by the actions of employees, government agencies and companies. According to the 2018 Global Business Ethics Survey, conducted by the Ethics & Compliance Initiative, "when organizations prioritize integrity, employees are: less likely to feel pressure to violate ethics standards; less likely to observe misconduct; more likely to report misconduct they observe; and, less likely to experience retaliation for reporting."[1]

Assistant Attorney General Brian A. Benczkowski summed up the case for compliance well in his Keynote Address at the Ethics and Compliance Initiative 2019 Annual Impact Conference:

> The importance of corporate compliance cannot be overstated . . . [A] company's compliance program is the first line of defense that prevents the misconduct from happening in the first place. And if done right, it has the ability to keep the company off [the DOJ's] radar screen entirely. In fact, of all of the Principles of Prosecution of Business Organizations that prosecutors are instructed to consider by the Justice Manual in determining an appropriate resolution of a corporate case, an effective compliance program is the only principle that has the ability to prevent the crime from occurring in the first place.[2]

---

[1] Ethics & Compliance Initiative, Global Business Ethics Survey: The State of Ethics & Compliance in the Workplace (March 2018), *available at* https://www.ethics.org/download-the-2018-global-business-ethics-survey/.

[2] Brian A. Benczkowski, Assistant Attorney General, Keynote Address at the Ethics and Compliance Initiative Annual Impact Conference (Apr. 30, 2019), *available at* https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-keynote-address-ethics-and.

CRAVATH, SWAINE & MOORE LLP