Corporate Compliance Survey

*By Paul E. McGreal**

This is the sixth survey from the Corporate Compliance Committee.[1] This survey summarizes significant legal developments from the last year regarding corporate compliance and ethics programs, which consist of an organization's code of conduct, policies, and procedures designed to achieve compliance with applicable legal regulations and internal ethical standards.[2] For an overview and introduction to the subject, as well as updates from prior years, please see the prior surveys.[3] This update assumes familiarity with the background and overview discussed there.

As in past surveys, Part I reviews developments regarding the United States Sentencing Guidelines for the sentencing of organizations (the "Guidelines");[4] Part II reviews significant regulatory developments; and Part III reviews significant case law developments. And in recognition of the increasingly global nature of compliance, this survey adds a Part IV devoted to significant international developments.

I. Organizational Sentencing Guidelines

The United States Sentencing Commission ("Commission") has proposed changes to the organizational Guidelines that strengthen and clarify the role of corporate compliance and ethics programs.[5] Unless Congress takes action to the contrary, the proposed amendments will go into effect on November 1, 2010.[6]

* Professor of Law, Southern Illinois University School of Law.

1. This survey incorporates background and related discussions from the prior surveys. *See* Corporate Compliance Comm., Am. Bar Ass'n Section of Bus. Law, *Corporate Compliance Survey*, 60 Bus. Law. 1759 (2005) [hereinafter *Survey I*]; Corporate Compliance Comm., Am. Bar Ass'n Section of Bus. Law, *Corporate Compliance Survey*, 61 Bus. Law. 1645 (2006); Corporate Compliance Comm., Am. Bar Ass'n Section of Bus. Law, *Corporate Compliance Survey*, 63 Bus. Law. 195 (2007) [hereinafter *Survey III*]; Paul E. McGreal, *Corporate Compliance Survey*, 64 Bus. Law. 253 (2008); Paul E. McGreal, *Corporate Compliance Survey*, 65 Bus. Law. 193 (2009) [hereinafter *Survey V*].

2. While compliance programs can take an even broader view, managing all of the organization's risks, I focus here on legal compliance.

3. *See supra* note 1.

4. U.S. Sentencing Guidelines Manual § 8B2.1 (Nov. 2009), *available at* http://www.ussc.gov/2009guid/GL2009.pdf [hereinafter USSG].

5. Sentencing Guidelines for United States Courts, 75 Fed. Reg. 27388 (May 14, 2010).

6. *Id*. at 27388.

The proposals touch on two main issues: (1) how an organization should respond to discovery of wrongdoing, and (2) whether an organization should be eligible for the sentencing credit when high-level or substantial-authority personnel participate in the wrongdoing.[7] Each proposal is discussed in turn.[8]

A. Responding to Corporate Wrongdoing

The proposed amendments clarify the steps that an organization should take in response to an incident of wrongdoing. The existing Guidelines on the subject provide as follows: "After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program."[9] Under this provision, an appropriate response has two essential elements: remedy the wrongdoing itself, then take steps to prevent similar misconduct in the future. The proposed amendments elaborate on the measures that an organization should take under each element.

First, the proposed Guidelines suggest steps for remedying the wrongdoing:

> First, the organization should respond appropriately to the criminal conduct. The organization should take reasonable steps, as warranted under the circumstances, to remedy the harm resulting from the criminal conduct. These steps may include, where appropriate, providing restitution to identifiable victims, as well as other forms of remediation. Other reasonable steps to respond appropriately to the criminal conduct may include self-reporting and cooperation with authorities.[10]

Note that each step is phrased in optional language: "as warranted under the circumstances," "may include," and "may include, where appropriate." That said, by listing these items in the application notes, the Commission likely ensured that organizations will specifically consider each form of response and articulate reasons for the decision whether to do so.

Second, the proposed Guidelines amendments direct an organization to prevent future misconduct:

> Second, the organization should act appropriately to prevent further similar criminal conduct, including assessing the compliance and ethics program and making

7. *Id*. at 27394. The organizational Guidelines were also amended to "remove[] the distinction between conditions of probation imposed solely to enforce a monetary penalty and conditions of probation imposed for any other reason so that all conditional probation terms are available for consideration by the court in determining an appropriate sentence." *Id*. at 27395. That amendment is outside the scope of this survey and, therefore, is not discussed.

8. For a discussion of the history and context of the proposed amendments, as well as their likely effect, see Win Swenson & Joe Murphy, *Changes Coming in Company Compliance Programs: The U.S. Sentencing Commission Adjusts the Rules*, 8 Corp. Accountability Rep. (BNA) 722 (May 7, 2010).

9. USSG § 8B2.1(b)(7).

10. Sentencing Guidelines for United States Courts, 75 Fed. Reg. at 27394.

> modifications necessary to ensure the program is effective. The steps taken should be consistent with subsections (b)(5) and (c) and may include the use of an outside professional advisor to ensure adequate assessment and implementation of any modifications.[11]

This guidance is implicit in the current Guidelines, which require an organization to assess periodically the effectiveness of compliance and ethics programs.[12] Discovery of misconduct is a logical time for such an assessment, and the proposed application note makes this clear. The additional suggestion of "an outside professional advisor" as a step an organization "may" take, while new to the Guidelines, is consistent with other compliance guidance. The gist is that someone independent from the compliance and ethics program, whether from within or outside the organization, should bring an objective eye to assessing the effectiveness of the compliance and ethics program. That is, those responsible for designing, implementing, and operating the compliance program ought not be the only ones to assess their handiwork. This guidance is consistent with compliance guidance in other areas, such as that for health care[13] and anti-money laundering programs.[14]

B. Expanded Sentencing Credit

The current Guidelines deny the three-point reduction in culpability score if either substantial-authority[15] or high-level personnel[16] of the organization "participated in, condoned, or was willfully ignorant of the offense."[17] The proposed amendments would permit the sentencing credit under those circumstances if an organization can make four showings:

---

11. *Id.*

12. USSG § 8B2.1(c).

13. *See, e.g.*, Publication of the OIG Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8987, 8993 n.35 (Feb. 23, 1998) ("By separating the compliance function from the key management positions . . . a system of checks and balances is established to more effectively achieve the goals.").

14. *See* Conducting Independent Reviews of Money Services Business Anti-Money Laundering Programs: Frequently Asked Questions, FIN-2006-G012 (Sept. 22, 2006), *available at* http://www.fincen.gov/statutes_regs/guidance/pdf/Guidance_MSB_Independent_Audits9-21.pdf.

15. USSG § 8A1.2 cmt. n.3(c) ("'Substantial authority personnel' means individuals who within the scope of their authority exercise a substantial measure of discretion in acting on behalf of an organization. The term includes high-level personnel of the organization, individuals who exercise substantial supervisory authority (e.g., a plant manager, a sales manager), and any other individuals who, although not a part of an organization's management, nevertheless exercise substantial discretion when acting within the scope of their authority (e.g., an individual with authority in an organization to negotiate or set price levels or an individual authorized to negotiate or approve significant contracts). Whether an individual falls within this category must be determined on a case-by-case basis.").

16. USSG § 8A1.2 cmt. n.3(b) ("'High-level personnel of the organization' means individuals who have substantial control over the organization or who have a substantial role in the making of policy within the organization. The term includes: a director; an executive officer; an individual in charge of a major business or functional unit of the organization, such as sales, administration, or finance; and an individual with a substantial ownership interest. 'High-level personnel of a unit of the organization' is defined in the Commentary to § 8C2.5 (Culpability Score).").

17. USSG § 8C2.5(f)(3)(A).

(i) The individual or individuals with operational responsibility for the compliance and ethics program (see § 8B2.1(b)(2)(C)) have direct reporting obligations to the governing authority or an appropriate subgroup thereof (e.g., an audit committee of the board of directors);
(ii) The compliance and ethics program detected the offense before discovery outside the organization or before such discovery was reasonably likely;
(iii) The organization promptly reported the offense to appropriate governmental authorities; and
(iv) No individual with operational responsibility for the compliance and ethics program participated in, condoned, or was willfully ignorant of the offense.[18]

Subsections (ii) through (iv) are relatively straightforward, as an effective compliance and ethics program should support early detection and self-reporting of wrongdoing, and would not brook participation of the organization's compliance professionals in the wrongdoing. Subsection (i), however, provides an important elaboration on the proper relationship between compliance and ethics officers and the board. First, the proposed amendment requires that in-house compliance personnel have "direct reporting obligations" to the board. The proposed application notes define that term as follows:

> [A]n individual has "direct reporting obligations" to the governing authority or an appropriate subgroup thereof if the individual has express authority to communicate personally to the governing authority or appropriate subgroup thereof (A) promptly on any matter involving criminal conduct or potential criminal conduct, and (B) no less than annually on the implementation and effectiveness of the compliance and ethics program.[19]

The direct reporting obligation, then, has three aspects. First, the authority to report must be "express," which strongly counsels organizations to document the reporting authority. Second, the authority must be to "communicate personally," which rules out either an indirect report through a superior or a mere paper report. And third, the reports must occur both regularly ("no less than annually") and in the event of criminal misconduct.

A second important aspect of the proposed Guidelines amendment is that the reporting authority must rest in "the individual or individuals with operational responsibility for the compliance and ethics program." Consequently, it is not enough that a chief compliance and ethics officer with high level oversight of the compliance and ethics program report to the board. Two commentators have explained that this requirement addresses the case where an organization designates the general counsel as chief compliance and ethics officer, and delegates operational responsibility to another official.[20] In that case, it is not enough that the general counsel report to the board—the director of compliance ethics must do so. Further, as noted above, the report must be made "personally," eliminating the possibility of a mere paper report.

18. Sentencing Guidelines for United States Courts, 75 Fed. Reg. 27388, 27394 (May 14, 2010).
19. *Id*.
20. *See* Swenson & Murphy, *supra* note 8, at 725.

II. Regulatory Developments

This part reviews two major compliance-related regulatory initiatives from the last year. I offer a brief description of each development; readers interested in more detail should consult the citations to relevant sources, most of which are available on the internet. The discussion is organized by agency.

A. State Health Care Compliance Program Mandates

Over the last decade, the Office of the Inspector General ("OIG") of the United States Department of Health and Human Services ("HHS") has issued elaborate compliance guidance to various segments of the health care industry. The HHS online compliance library includes guidance documents tailored to (among others) hospitals, clinical labs, home health agencies, third-party billing companies, durable medical equipment companies, hospices, nursing facilities, and pharmaceutical manufacturers.[21] While not promising specific credit for an ethics and compliance program, the OIG identifies several benefits it believes will result from implementing such programs: "The OIG believes a comprehensive compliance program provides a mechanism that addresses the public and private sectors' mutual goals of reducing fraud and abuse; enhancing health care provider operational functions; improving the quality of health care services; and reducing the cost of health care."[22] The OIG's compliance pitch tracks conventional wisdom: compliance programs can prevent wrongdoing and detect violations earlier, eliminating or reducing an organization's liability.[23]

During 2009, New York and Connecticut pushed beyond HHS's mere encouragement to require compliance and ethics programs for certain health care providers participating in their Medicare programs. First, New York added a section to its social services law in 2006 to include the compliance and ethics program requirement.[24] The section, which is reproduced in Appendix A, sets forth eight

21. *See, e.g.*, OIG Compliance Program Guidance for Ambulance Suppliers, 68 Fed. Reg. 14245 (Mar. 24, 2003); OIG Compliance Program for Individual and Small Group Physician Practices, 65 Fed. Reg. 59434 (Oct. 5, 2000); OIG Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8987 (Feb. 23, 1998).

22. OIG Compliance Program Guidance for Pharmaceutical Manufacturers, 68 Fed. Reg. 23731, 23732 (May 5, 2003).

23. The OIG does note, however, that a compliance program may influence agency enforcement decisions: "The OIG . . . will consider the existence of an *effective* compliance program that pre-dated any Governmental investigation when addressing the appropriateness of administrative penalties." OIG Compliance Program Guidance for Hospitals, 63 Fed. Reg. at 8988 n.2 (emphasis added).

24. N.Y. Soc. Serv. Law § 363-d (McKinney Supp. 2010). Interestingly, the law provides a safe harbor for organizations that have a compliance and ethics program that has been "accepted" as effective by HHS. *Id.* § 363-d.3(a). As an FAQ promulgated by the New York Office of Medicaid Inspector General explains, HHS does not certify or accept provider compliance and ethics programs:

> IS THERE AN EXCEPTION TO THE MANDATORY COMPLIANCE LAW?
>
> The Mandatory Compliance Law provides that "a compliance program that is accepted by the United States Department of Health and Human Services Office of Inspector General and remains in compliance with the standards promulgated by such office shall be deemed in compliance

components of an ethics and compliance program that parallel the seven steps of the federal organizational sentencing Guidelines.[25] For example, the law requires covered health care organizations to "designate an employee vested with responsibility for the day-to-day operation of the compliance program," and that "such employee shall report directly to the entity's chief executive or other senior administrator and shall periodically report directly to the governing body on the activities of the compliance program."[26] This parallels the federal sentencing Guidelines requirements that an organization appoint personnel with oversight of the compliance program, and that those personnel periodically report to the organization's governing authority.[27] The statute directs the state's Office of Medicaid Inspector General ("OMIG") to specify the health care organizations to which the mandate applies, and to "create and make available on its website guidelines, which may include a model compliance program, that reflect the requirements of this section."[28]

In June 2009, the New York OMIG published a final rule implementing the statute's compliance and ethics program mandate.[29] The rule applies the mandate to providers who receive $500,000 or more in Medicaid reimbursements from the State of New York.[30] Notably, however, the rule does not elaborate on the eight steps found in the statute, except to identify six specific compliance risks that the program must address.[31] In response to comments critical of the lack of guidance, the OMIG explained that additional guidance would be forthcoming in the form of industry-specific documents:

> We believe the specific questions posed by commenters relating to the eight elements required to be incorporated into a provider's compliance program pursuant to SSL 363-d are more appropriately addressed in the provider specific compliance guidance. The OMIG has been and continues to work closely with specific segments of the provider community to develop industry specific provider compli-

with the provision of this law." However, the US HHS OIG does not review and "accept" provider compliance plans. A compliance program may be a part of more comprehensive compliance activities so long as the minimum requirements of the law and implementing regulations are met.

Mandatory Provider Compliance Programs: Frequently Asked Questions, N.Y. ST. OFFICE MEDICAID INSPECTOR GEN., http://www.omig.state.ny.us/data/content/view/79/65 (last visited Sept. 11, 2010) [hereinafter *Mandatory Provider Compliance Programs FAQs*].

25. N.Y. SOC. SERV. LAW § 363-d.2.

26. *Id*. § 363-d.2(b).

27. USSG § 8B2.1(b)(2)(C) (2009).

28. N.Y. SOC. SERV. LAW § 363-d.2.

29. 25 N.Y. Reg. 7 (June 24, 2009), *available at* http://www.dos.state.ny.us/info/register/2009/jun24/pdfs/rules.pdf; N.Y. COMP. CODES R. & REGS. tit. 18, § 521 (2009).

30. N.Y. COMP. CODES R. & REGS. tit. 18, § 521.2(b).

31. Under section 521.3(a), "Required providers' compliance programs shall be applicable to:

(1) billings; (2) payments; (3) medical necessity and quality of care; (4) governance; (5) mandatory reporting; (6) credentialing; and (7) other risk areas that are or should with due diligence be identified by the provider."

> ance guidance to allow flexibility for a provider to develop a program appropriate to its characteristics.[32]

And while the statute suggests that the OMIG may accompany this guidance with a model compliance and ethics program, the OMIG has no plans to provide such a model.[33]

The OMIG regulations require covered providers to file an annual certification of compliance with the mandatory compliance and ethics program requirement.[34] While the rule does not designate who must make the annual certification, the OMIG has published an FAQ on its website that provides the following guidance: "The OMIG strongly encourages that someone from senior management (other than the compliance officer) or a member of the governing authority sign the certification as an indication that the provider's compliance efforts and responsibilities extend beyond the compliance officer."[35]

In unofficial commentary, a representative of the OMIG has emphasized that the office will examine whether an organization's board has set an appropriate tone at the top for an effective compliance and ethics program.[36] And the FAQ makes clear that both the statute and rule arm the OMIG with the power to exclude a non-complying person or organization from participation in Medicaid.[37] For example, this would include a physician who serves on the board of a covered health care provider, and who does not adequately exercise her duty of oversight of the provider's health care compliance and ethics program.[38]

In June 2010, Connecticut enacted a statute requiring medical device and pharmaceutical companies operating in the state to adopt a code of conduct and compliance and ethics program by January 1, 2011.[39] This law differs from the New York law in several respects. First, the law applies both more broadly and narrowly than the New York law. On the one hand, the Connecticut law is broader because it is not limited to Medicaid participants. On the other hand, the Connecticut law is comparatively quite narrow because it applies to only two segments of the health care industry—medical device and pharmaceutical firms.

---

32. 25 N.Y. Reg. 10 (June 24, 2009).
33. *See Mandatory Provider Compliance Programs FAQs*, *supra* note 24.
34. N.Y. Comp. Codes R. & Regs. tit. 18, § 521.3(b) ("[D]uring the month of December each year . . . a required provider shall certify to the department, using a form provided by the Office of the Medicaid Inspector General on its website, that a compliance program meeting the requirements of this Part is in place."). The initial certification was due December 31, 2009. *See Mandatory Provider Compliance Programs FAQs*, *supra* note 24.
35. *See Mandatory Provider Compliance Programs FAQs*, *supra* note 24.
36. *See State of New York Mandates Hospital Compliance Programs*, 17 Prevention Corp. Liability (BNA) 95, 96 (Aug. 17, 2009) (quoting New York Medicaid Inspector General James Sheehan).
37. *See Mandatory Provider Compliance Programs FAQs*, *supra* note 24.
38. *See State of New York Mandates Hospital Compliance Programs*, *supra* note 36, at 96.
39. Act of June 8, 2010, Pub. Act No. 10-117, § 94 (West, Westlaw through 2010 February Regular Sess. and June Special Sess.) (concerning revisions to public health related statutes and the establishment of the health information technology exchange of Connecticut).

A second difference is that the Connecticut law does not specify the required compliance measures, but rather codifies compliance standards established by third parties. For the mandatory code of ethics, the law requires firms to "adopt and implement a code that is consistent with, and minimally contains all of the requirements prescribed in, the Pharmaceutical Research and Manufacturers of America's 'Code on Interaction with Healthcare Professionals' or AdvaMed's 'Code of Ethics on Interactions with Health Care Professionals' as such codes were in effect on January 1, 2010."[40] For the mandatory compliance and ethics program, firms must "adopt a comprehensive compliance program in accordance with the guidelines provided in the 'Compliance Program Guidance for Pharmaceutical Manufacturers' dated April, 2003 and issued by the United States Department of Health and Human Services Office of Inspector General."[41] The state may punish lapses with a fine up to $5,000.[42]

B. Federal Trade Commission Red Flags Rule

The Fair and Accurate Credit Transactions Act of 2003 ("FACT Act") requires certain federal agencies, including the Federal Trade Commission ("FTC"), to "prescribe regulations requiring each financial institution and each creditor to establish reasonable policies and procedures . . . to identify possible risks to account holders or customers" of "identity theft with respect to account holders at, or customers of, such entities."[43] The statute also directs the FTC to "establish and maintain guidelines" for such policies and procedures, and to "update such guidelines as often as necessary."[44] In November 2007, the FTC and other agencies published a final rule providing the required guidance.[45] Because the rule addresses policies and procedures for identifying risks, or "red flags," of identity theft, the rule was dubbed the "Red Flags Rule." An appendix to the rule identifies specific red flags of identity theft, and outlines compliance measures to identify the red flags and prevent potential identify theft.[46]

Since the Red Flags Rule was announced, the main controversy has been over the scope of its application. The underlying statute applies to any "financial institution" or "creditor," and the Red Flags Rule refers to a definition of those terms in a separate statute,[47] adding only that creditors "include lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and

40. *Id.* § 94(a).
41. *Id.* § 94(b).
42. *Id.* § 94(c).
43. FACT Act § 114, 15 U.S.C. § 1681m(e)(1)(A), (B) (2006).
44. *Id.* § 114, § 1681m(e)(1)(A).
45. Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63718 (Nov. 9, 2007) (to be codified at 12 C.F.R. pts. 41, 222, 334, 364, 571 & 717 and 16 C.F.R. pt. 681).
46. 16 C.F.R. pt. 681 app. A (2009).
47. *See* Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. at 63722 (referring to the statutory definitions of "financial institution" and "creditor" in 15 U.S.C. § 1681a(r)(5)).

telecommunications companies."[48] Lawyers, accountants, and doctors, among others, were unclear whether they fell within this meaning of "creditor." Because of this confusion, the FTC delayed the Rule's effective date from November 2008 to May 2009, further explaining that a "creditor" included "entities that defer payment for goods or services."[49] When this clarification still left doubt, the FTC again delayed enforcement, this time until August 2009.[50] In doing so, the FTC defined "creditor" in a way that finally made clear that lawyers and other professionals fell within the rule: "[A] retailer or service provider that, on a regular basis, allows its customers to make purchases or obtain services and then bills them for payment at the end of each month would be a creditor . . . ."[51] The American Bar Association filed suit to have a federal court declare that the FTC lacked authority to apply the Red Flags Rule to lawyers,[52] and the FTC again delayed enforcement, this time until November 2009.[53]

In December 2009, the United States District Court for the District of Columbia held that the FTC did not have authority to apply the Red Flags Rule to the legal profession.[54] Based on its reading of the relevant statutory text, regulatory background, and surrounding case law, the district court concluded that the term "creditor" does not include professionals, like attorneys, who bill their clients after providing their services.[55] For attorneys, such billing is often the only practical way to do business, and not a true extension of credit.[56] After the ruling, the FTC delayed enforcement yet again, until June 1, 2010,[57] while the accounting and medical professions mounted legal challenges of their own.[58] The FTC has appealed the district court's ruling to the federal court of appeals, and Congress has introduced legislation that would clarify application of the Red Flags Rule.[59] In

48. 16 C.F.R. § 681.1(b)(5) (2009).

49. Press Release, Fed. Trade Comm'n, FTC Will Grant Six-Month Delay of Enforcement of 'Red Flags' Rule Requiring Creditors and Financial Institutions to Have Identity Theft Prevention Programs (Oct. 22, 2008), *available at* http://www.ftc.gov/opa/2008/10/redflags.shtm.

50. Press Release, Fed. Trade Comm'n, FTC Extended Enforcement Policy: Identity Theft Red Flags Rule, 16 C.F.R. § 681.1, at 1 n.3 (Apr. 30, 2009), *available at* http://www.ftc.gov/os/2009/04/P095406redflagsextendedenforcement.pdf.

51. *Id*.

52. *See* Complaint for Declaratory and Injunctive Relief, Am. Bar Ass'n v. FTC, No. 1:09-cv-01636-RBW (D.D.C. Aug. 27, 2009).

53. Press Release, Fed. Trade Comm'n, FTC Announces Expanded Business Education Campaign on 'Red Flags' Rule (July 29, 2009), *available at* http://www.ftc.gov/opa/2009/07/redflag.shtm.

54. Am. Bar Ass'n v. FTC, 671 F. Supp. 2d 64, 82 (D.D.C. 2009) ("Attorneys simply do not meet the overly broad definition of creditors adopted by the Commission."). The accounting and medical professions have also filed lawsuits seeking a similar judgment. *See* Complaint for Declaratory and Injunctive Relief, Am. Med. Ass'n v. FTC, No. 10-CV-00843 (D.D.C. May 21, 2010); Complaint for Declaratory and Injunctive Relief, Am. Inst. of Certified Pub. Accountants v. FTC, No. 1:09-cv-02116 (D.D.C. Nov. 10, 2009).

55. *Am. Bar Ass'n*, 671 F. Supp. 2d at 82.

56. *Id*. at 75.

57. Press Release, Fed. Trade Comm'n, FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule (Oct. 30, 2009), *available at* http://www.ftc.gov/opa/2009/10/redflags.shtm.

58. *See supra* note 54.

59. *See* H.R. 3763, 111th Cong. § 1 (2009); S. 3416, 111th Cong. § 1 (2009).

the face of this uncertainty, and at the request of Congress, the FTC has, as of this writing, now postponed enforcement of the Red Flags Rule until December 31, 2010.[60] So, the end to this ongoing saga must await next year's survey. In the interim, businesses that clearly fall within the Rule's scope should implement the required red flags compliance measures, as none of the pending litigation or legislation would void the Red Flags Rule in its entirety.

III. Case Law Standards

Part III reviews compliance-related case law developments in state corporate law[61] and selected areas of federal law.[62] Section A reviews developments regarding the board's duty, first discussed in *In re Caremark International Inc. Derivative Litigation*,[63] to oversee a corporation's legal compliance efforts. Section B then reviews federal cases covering sexual harassment.

A. The *Caremark* Claim

In dicta in its 1996 decision *In re Caremark International Inc. Derivative Litigation*, the Delaware Court of Chancery addressed the board's duty to oversee a corporation's legal compliance efforts.[64] As part of its duty to monitor, the board must make good-faith efforts to ensure that a corporation has adequate reporting and information systems.[65] The court described a claim for breach of that duty as "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment,"[66] with liability attaching only for "a sustained or systematic failure of the board to exercise oversight" or "an utter failure to attempt to assure a reasonable information and reporting system exists."[67]

Since the decision, this Delaware dicta has morphed into what has become known as a *Caremark* claim, as federal and state courts, both within and outside Delaware, have recognized a cause of action against boards for failing to take minimal steps to achieve legal compliance.[68] As the phrases "utter failure" and

60. Press Release, Fed. Trade Comm'n, FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule (May 28, 2010), *available at* http://www.ftc.gov/opa/2010/05/redflags.shtm.

61. *See generally* Charles M. Elson & Christopher J. Gyves, *In re* Caremark*: Good Intentions, Unintended Consequences*, 39 Wake Forest L. Rev. 691 (2004); H. Lowell Brown, *The Corporate Director's Compliance Oversight Responsibility in the Post* Caremark *Era*, 26 Del. J. Corp. L. 1 (2001).

62. *See generally* Rebecca S. Walker, *What We Can Learn About Effective Compliance Policies from Recent Employment Discrimination Cases*, Ethikos (July/Aug. 2000), http://www.ethikospublication.com/html/discrimination.html.

63. 698 A.2d 959 (Del. Ch. 1996). The inaugural survey discusses the background and compliance context of this case. *See Survey I*, *supra* note 1, at 1773–76.

64. *Caremark*, 698 A.2d at 970–71.

65. *Id*. at 967–70.

66. *Id*. at 967.

67. *Id*. at 971.

68. For a more detailed discussion of the *Caremark* case and development of the *Caremark* claim, see Brown, *supra* note 61, at 7–32. For a critique of *Caremark*'s impact, see Elson & Gyves, *supra* note 61, at 691–706.

"systematic failure" suggest, a board's *Caremark* duty is relatively low.[69] Only egregious lapses breach this duty, such as when board members ignore obvious red flags signaling illegal behavior,[70] fail to appoint or convene an audit committee,[71] or do not address obvious concerns such as large loans to corporate insiders.[72]

In *Stone ex rel. AmSouth Bancorporation v. Ritter*, the Delaware Supreme Court formally embraced the *Caremark* claim.[73] The court both confirmed the elements of a *Caremark* duty and clarified that breach of that duty constitutes a breach of the director's duty of loyalty:

> We hold that *Caremark* articulates the necessary conditions predicate for director oversight liability: (a) the directors 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. In either case, imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations. Where directors fail to act in the face of a known duty to act, thereby demonstrating a conscious disregard for their responsibilities, they breach their duty of loyalty by failing to discharge that fiduciary obligation in good faith.[74]

The court in *Stone*, then, adopted the *Caremark* duty and restated it as having two components. First, there is a director's *initial duty* to address compliance and ethics.[75] The director breaches this branch of the *Caremark* duty by failing to take *any* action directed toward establishing a compliance and ethics program.[76]

Second, there is an *ongoing duty* to address compliance and ethics.[77] The director breaches this branch of the *Caremark* duty if she learns of a specific gap or weakness in the organization's compliance and ethics program, but takes no action to address that failing.[78] For example, a director may actually know of a new regulatory scheme or requirement that directly affects the business of her corporation, and then fail to inquire whether the organization is taking measures to comply with the new law. Or a board that charged management with implementing a compliance and ethics program may never receive or request reports on the design, implementation, and operation of the program. Note that in both these examples, the board member's failure is to not inquire of management; the

69. *See Caremark*, 698 A.2d at 971.

70. *See, e.g.*, McCall v. Scott, 250 F.3d 997, 999 (6th Cir. 2001); Benjamin v. Kim, No. 95 CIV. 9597 (LMM), 1999 WL 249706, at *13–14 (S.D.N.Y. Apr. 28, 1999) (quoting Graham v. Allis-Chalmers Mfg. Co., 188 A.2d 125, 130 (Del. 1963)).

71. *See, e.g.*, Guttman v. Huang, 823 A.2d 492, 506–07 (Del. Ch. 2003) (remarking in dicta that failure to have an audit committee would be the type of egregious failing that would support a *Caremark* claim).

72. *See, e.g.*, Pereira v. Cogan, 294 B.R. 449, 532–33 (S.D.N.Y. 2003), *vacated & remanded sub nom.* Pereira v. Farace, 413 F.3d 330 (2d Cir. 2005), *cert. denied*, 547 U.S. 1147 (2006).

73. 911 A.2d 362 (Del. 2006).

74. *Id.* at 370 (footnotes omitted).

75. *Id.*

76. *See id.*

77. *Id.*

78. *See id.*

board member need not actually design or implement the program itself. This is because the director's duty is one of oversight, and the board may rely on management in satisfying this duty.

The Delaware courts have been demanding of plaintiffs who allege breach of either component of the *Caremark* duty—the initial or ongoing duty of oversight. First, as to breach of a director's initial duty, the reported decisions require the plaintiff to plead that the director took no actions related to compliance and ethics. A prior survey discussed a case where the plaintiff adequately pled that the directors consciously did *nothing* to prevent legal wrongdoing.[79] In that case, the directors were described as "stooges" for the corporation's president, who was looting the corporation of its assets.[80] Because the directors literally did nothing at all—never even met—the inference of conscious disregard was inescapable.[81] Indeed, given that the directors were "stooges," it is possible they did not know a duty of oversight existed.[82] The court's decision implies, then, that conscious disregard does not require that the director was specifically aware of her *Caremark* duty. Of course, this makes sense—directors ought not to be rewarded for ignorance of the fiduciary duties they voluntarily undertake as a director.

The pleading standard is also quite rigorous when a plaintiff alleges breach of the ongoing duty to oversee compliance and ethics. In those cases, the Delaware courts have confirmed the high threshold for pleading director *Caremark* liability: plaintiffs must plead specific facts that show the directors knowingly disregarded their ongoing duty to oversee the organization's compliance and ethics program.[83] The courts in these same cases have consistently held that a plaintiff will *not* meet this burden by simply pleading that the organization committed egregious or widespread wrongdoing; thus, the directors *must have* known about and ignored the legal problem.[84] In short, the degree or scope of wrongdoing when standing alone, however severe, will not give rise to an inference that directors were conscious of the organization's legal problems. Instead, the plaintiff must allege facts showing that the directors actually knew of the wrongdoing or utterly failed to address potential wrongdoing.

79. *See Survey III*, *supra* note 1, at 212–13.

80. ATR-Kim Eng Fin. Corp. v. Araneta, No. 489-N, 2006 WL 3783520, at * 1, *19 (Del. Ch. Dec. 21, 2006).

81. *See id.* at *21.

82. For examples of the directors' actions that led the court to identify them as "stooges," see *id.* at *20–21.

83. *See Survey V*, *supra* note 1, at 207.

84. *See* Stone *ex rel.* AmSouth Bancorporation v. Ritter, 911 A.2d 362, 373 (Del. 2006) ("The lacuna in the plaintiffs' argument is a failure to recognize that the directors' good faith exercise of oversight responsibility may not invariably prevent employees from violating criminal laws, or from causing the corporation to incur significant financial liability, or both . . . ."); Desimone v. Barrows, 924 A.2d 908, 940 (Del. Ch. 2007) ("Delaware courts routinely reject the conclusory allegation that because illegal behavior occurred, internal controls must have been deficient, and the board must have known so."); Guttman v. Huang, 823 A.2d 492, 506–07 (Del. Ch. 2003) ("Their conclusory complaint is empty of the kind of fact pleading that is critical to a *Caremark* claim, such as contentions that . . . the audit committee had clear notice of serious accounting irregularities and simply chose to ignore them or, even worse, to encourage their continuation.").

An Illinois state court of appeals case from the last year illustrates how the pleading standard works. *Sherman v. Ryan* was a shareholder derivative suit against the board of directors of the insurance brokerage firm Aon Corporation.[85] The shareholders alleged that Aon had engaged in the practice of collecting "contingent commissions," which it described as "payments made from insurance carriers to the brokers, based on volume and profitability of business passed on from the broker to a particular carrier."[86] The shareholders further alleged that the "contingent commissions encouraged Aon to send business to carriers that offered the highest commission, not necessarily those most suitable to meet the needs of Aon's clients."[87] When this practice came to light, Aon faced a series of state and federal civil lawsuits and government enforcement actions resulting in settlements and fines in the hundreds of millions of dollars.[88]

Because the brokerage firm was a Delaware corporation, the Illinois court applied Delaware corporate law.[89] The case was decided on the issue of demand futility—the shareholders had not demanded that the board bring suit on behalf of the corporation, and so Delaware law required the shareholders to show that the demand was excused because it would have been futile to do so.[90] Demand would be futile if the board members were conflicted on the issue of bringing suit, and such a conflict would arise if the plaintiff's allegations raised a "substantial likelihood" that the board members would be personally liable.[91] One could hardly expect board members to fairly consider a shareholder demand that the board sue itself.

As one of their claims, the shareholders in *Sherman* alleged that Aon's board members violated their *Caremark* duty because they "failed to act and properly supervise Aon in the face of repeated 'red flags' indicating problems."[92] This claim was a breach of the board's ongoing duty to monitor, and not the initial duty to tend to compliance. Indeed, the shareholders acknowledged that the board had satisfied its initial *Caremark* duty when their complaint alleged that Aon had established a compliance and ethics program.[93] The question was whether the board had subsequently ignored red flags that the practice of contingent commissions would result in legal liability.[94] Specifically, the shareholders alleged that two private class action lawsuits based on the contingent commission practice put Aon's board on notice that the practice was suspect.[95]

The court concluded that the "spate of private litigation" was not enough to raise a *Caremark* red flag regarding the contingent commission practice.[96] The

85. 911 N.E.2d 378 (Ill. App. Ct. 2009).
86. *Id.* at 385.
87. *Id.*
88. *Id.* at 386–88.
89. *Id.* at 389.
90. *Id.* at 391.
91. *Id.*
92. *Id.* at 394.
93. *Id.* at 395.
94. *Id.* at 394.
95. *Id.* at 394–95.
96. *Id.* at 394.

court rested this conclusion on two factors. First, the class action was not certified until "shortly before Aon stopped accepting contingent commissions," and the practice had "ceased altogether" by the time the cases had settled.[97] Second, the contingent commission practice stopped soon after government regulators "showed any interest in contingent commissions."[98] These two factors suggest a threshold for when litigation constitutes a *Caremark* "red flag" that spurs board action. To start, the government's commitment of enforcement resources is a more serious red flag of potential wrongdoing than is a mere private lawsuit, which could be anything from a simple nuisance suit to a bet-the-company case. And this ties in to the second factor—the private lawsuit becomes a stronger signal of possible liability once the case passes a crucial milestone such as class certification. So, while the Aon board was not found to have breached its ongoing *Caremark* duty, the case strongly suggests that the board, or a board committee, ought to monitor ongoing private litigation to determine when a lawsuit evolves into a full-blown red flag.

B. Sexual Harassment: The *Ellerth*/*Faragher* Affirmative Defense

All organizations face the threat of sexual harassment liability and so should take measures to come within the affirmative defense recognized by the U.S. Supreme Court in *Burlington Industries, Inc. v. Ellerth*[99] and *Faragher v. City of Boca Raton*.[100] The Court in *Ellerth* and *Faragher* held that employers with effective compliance measures could avoid vicarious liability for sexual harassment committed by their supervisory[101] employees.[102] If the sexual harassment did not result in a tangible employment action, such as firing, demotion, or reduction of pay, the employer can avoid vicarious liability by pleading and proving a two-element affirmative defense: "(a) that the employer exercised reasonable care to prevent and correct promptly any sexually harassing behavior, and (b) that the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid harm otherwise."[103] Note that "reasonable care to prevent and correct promptly" the harassment—basically, a compliance program—is a necessary but not sufficient condition of the affirmative defense. *Even if* the employer has a state-of-the-art sexual harassment compliance program,

97. *Id*.
98. *Id*.
99. 524 U.S. 742 (1998).
100. 524 U.S. 775 (1998).
101. For a discussion of who counts as a supervisory employee, see Stephanie Ann Henning Blackman, Note, *The* Faragher *and* Ellerth *Problem: Lower Courts' Confusion Regarding the Definition of "Supervisor,"* 54 Vand. L. Rev. 123 (2001). For co-worker sexual harassment, the employer is vicariously liable only if it was negligent in detecting or remedying the harassment. *See Faragher*, 524 U.S. at 799 (describing lower courts as "uniformly judging employer liability for co-worker harassment under a negligence standard").
102. *Faragher*, 524 U.S. at 807–08; *Ellerth*, 524 U.S. at 764–65.
103. *Faragher*, 524 U.S. at 807.

the affirmative defense fails if the victim abided by the organization's program. Ironically, then, vicarious liability attaches despite the compliance program working precisely as intended.[104]

A case from the last year sheds light on how important it is for an organization to ensure that its supervisors are adequately integrated into the letter and spirit of its compliance and ethics program. *Whitten v. Fred's, Inc*.[105] involved a sexual harassment claim by a female assistant manager who was transferred from one work location to another. While the plaintiff asserted only a state law claim, the court of appeals looked to federal law in deciding the case.[106] The assistant manager alleged that she was verbally and physically harassed by the supervisor at the new location.[107] When the assistant manager complained about the harassment to the district manager, the district manager allegedly told her that "she was overreacting and that she should go on to work that day as if nothing had happened."[108] The employer moved for summary judgment, arguing that the fact it had a written sexual harassment policy established the *Ellerth/Faragher* defense as a matter of law.[109] The court of appeals rejected this argument, holding that the supervisor's response raised a genuine issue of material fact as to whether the employer acted reasonably.[110]

Whitten helpfully illustrates two points that should be conventional wisdom among compliance and ethics officers. First, a mere written policy does not ensure that an organization has an effective compliance and ethics program; an organization's employees must put the policies into practice every day. Second, employers must take special care in selecting and training supervisors. The employee alleged, and the employer could not conclusively disprove, that her supervisor dismissed her sexual harassment complaint. In other words, the supervisor did not document a proper response to the sexual harassment complaint, leaving the employer open to the argument that its sexual harassment compliance and ethics program was not reasonable.

IV. International Developments

Part IV examines two international compliance developments from the last year. Section A discusses anti-corruption compliance developments both in the

104. For a fuller discussion of these cases, see *Survey I*, *supra* note 1, at 1773–76.

105. 601 F.3d 231 (4th Cir. 2010).

106. *Id.* at 242 ("While there are no published opinions from South Carolina's appellate courts applying the substantive protections of the South Carolina Human Affairs Law to a claim of discrimination, the Supreme Court of South Carolina has stated that the act 'essentially follows the substantive structure of Title VII' and that Title VII cases 'are certainly persuasive if not controlling in construing the Human Affairs Law.' . . . Accordingly, we look to federal law for guidance when considering Whitten's claims. (quoting Orr v. Clyburn, 290 S.E.2d 804, 806 (S.C. 1982))).

107. *Id.* at 236.

108. *Id.* at 237.

109. Memorandum in Support of Defendant's Motion to Dismiss and for Summary Judgment at 25, Whitten v. Fred's, Inc., No. 08-cv-0218-HMH-BHH, 2008 WL 7147259 (D.S.C. Aug. 19, 2008).

110. *Whitten*, 601 F.3d at 251.

United States and abroad. Section B reviews the continued development of European Union ("EU") law on data privacy and whistleblower hotlines.

A. Global Anti-Corruption Laws

1. Foreign Corrupt Practices Act

The Foreign Corrupt Practices Act ("FCPA") criminalizes bribery of a foreign government official to obtain or retain business.[111] The FCPA applies both when an organization directly makes the forbidden payment to a foreign government official, and when the organization makes a payment to a third party (such as an agent or contractor) *knowing* that the third party will then make a forbidden payment to a foreign government official.[112] "Knowing" is defined to include circumstances where "a person is aware of a high probability of the existence of [the forbidden payment], unless the person actually believes that such circumstance does not exist."[113] Thus, a company or individual may be deemed to "know" of an agent's bribe if the company was "aware of a high probability" that a bribe might be made.[114] Such awareness could exist when an agent's activities raise red flags, such as a request for payment in cash or under an assumed name, a higher than usual commission, or a refusal to document expense reimbursement requests.[115] To avoid a finding that the organization "knew" such an agent was making bribes, the organization should implement compliance controls to prevent and detect agent misconduct.[116]

---

111. Foreign Corrupt Practices Act of 1977, Pub. L. No. 95-213, § 103(a), 91 Stat. 1494, 1495–96 (codified as amended at 15 U.S.C. § 78dd-1 (2006)).

112. FCPA § 103(a), 15 U.S.C. § 78dd-1(a)(3).

113. 15 U.S.C. § 78dd-1(f)(2)(B).

114. *Id.*

115. The DOJ has the following list of red flags:

> [U]nusual payment patterns or financial arrangements, a history of corruption in the country, a refusal by the foreign joint venture partner or representative to provide a certification that it will not take any action in furtherance of an unlawful offer, promise, or payment to a foreign public official and not take any act that would cause the U.S. firm to be in violation of the FCPA, unusually high commissions, lack of transparency in expenses and accounting records, apparent lack of qualifications or resources on the part of the joint venture partner or representative to perform the services offered, and whether the joint venture partner or representative has been recommended by an official of the potential governmental customer.

Fraud Section, U.S. Dep't of Justice, Foreign Corrupt Practices Act: Lay-Person's Guide to FCPA 4 (2010), *available at* http://www.justice.gov/criminal/fraud/fcpa/docs/lay-persons-guide.pdf.

116. *Id.* The DOJ also states:

> To avoid being held liable for corrupt third party payments, U.S. companies are encouraged to exercise due diligence and to take all necessary precautions to ensure that they have formed a business relationship with reputable and qualified partners and representatives. Such due diligence may include investigating potential foreign representatives and joint venture partners to determine if they are in fact qualified for the position, whether they have personal or professional ties to the government, the number and reputation of their clientele, and their reputation with the U.S. Embassy or Consulate and with local bankers, clients, and other business associates.

Id.

This last year saw two notable interpretations of the FCPA. First, the U.S. District Court for the Southern District of New York issued an opinion applying several FCPA provisions to a businessperson's actions during the privatization of the state-owned oil company in Azerbaijan. Second, the U.S. Department of Justice issued an opinion procedure release that provided guidance for companies that provide product samples to their government customers. This section addresses each development in turn.

First, a federal district court interpreted several provisions of the FCPA in the criminal prosecution in *United States v. Kozeny*.[117] At the outset of its opinion, the district court summarized the basic facts of what it called a "complex" case:

> SOCAR is the state-owned oil company of the Republic of Azerbaijan ("Azerbaijan"). In the mid-1990s, Azerbaijan began a program of privatization. The program gave the President of Azerbaijan, Heydar Aliyev, discretionary authority as to whether and when to privatize SOCAR. [Frederick] Bourke, co-defendant Viktor Kozeny, and others conspired to violate the FCPA by agreeing to make payments to Azeri officials to encourage the privatization of SOCAR and to permit them to participate in that privatization. The payments included, among other things, cash bribes, the gift of a two-thirds interest in the privatization venture, and assistance with obtaining a medical appointment, visas, and college admission in the United States.[118]

Bourke was tried and convicted on the charge of conspiracy to violate the FCPA.[119] The Second Circuit had previously defined the offense of conspiracy as follows:

> A conspiracy conviction under [18 U.S.C.] § 371 requires proof of three essential elements: (1) an agreement among two or more persons, the object of which is an offense against the United States; (2) the defendant's knowing and willful joinder in that conspiracy; and (3) commission of an overt act in furtherance of the conspiracy by at least one of the alleged co-conspirators.[120]

The government's theory of the case was that a group of businesspeople, of which Bourke was a member, had conspired to pay Azeri government officials in exchange for participation in the privatization of SOCAR, and that Bourke knew of the object of this conspiracy.[121] Bourke argued that he did not have the requisite knowledge to satisfy a conspiracy charge because he did not actually know whether specific bribes were ultimately paid to Azeri officials.[122] The district court rejected this argument, explaining that conspiracy does not require proof that the defendant knew of completion of the conspiracy:

> The Government must prove that Bourke had knowledge of the object of the conspiracy, which was to violate the FCPA, not that bribes had, in fact, been paid. Indeed, a defendant can be convicted of conspiracy even if the object of the conspiracy—in this

117. 664 F. Supp. 2d 369 (S.D.N.Y. 2009).
118. *Id.* at 372 (footnotes omitted).
119. *Id.*
120. United States v. Svoboda, 347 F.3d 471, 476 (2d Cir. 2003).
121. *See Kozeny*, 664 F. Supp. 2d at 374–75.
122. *Id.* at 374.

> case, the making of corrupt payments in return for the privatization of SOCAR—is never fully consummated.[123]

The district court then concluded that the trial evidence adequately supported a finding that Bourke knew of the object of the conspiracy to bribe Azeri officials.[124]

The district court also held that the government may properly receive an instruction on "conscious avoidance" to "satisfy the knowledge component of the intent to participate in the conspiracy."[125] A conscious avoidance instruction has two prerequisites:

> A conscious avoidance charge is proper "(i) when a defendant asserts the lack of some specific aspect of knowledge required for conviction and (ii) the appropriate factual predicate for the charge exists." A factual predicate exists when "the evidence is such that a rational juror may reach the conclusion beyond a reasonable doubt that the defendant was aware of a high probability of the fact in dispute and consciously avoided confirming that fact."[126]

The district court held that the predicate existed here because, first, Bourke contended that he did not know of the bribes that underlay the conspiracy, and second, Bourke knew of a high probability that bribes would be paid and then consciously avoided actually learning that fact.[127] The court noted several factors supporting its conclusion that Bourke was aware of a high probability that bribes would be paid: doing business in Azerbaijan was known to pose a high risk of corruption, Bourke's lawyer had referred to Azerbaijan as the "wild west" in Bourke's presence, Bourke was aware that his agent in Azerbaijan had committed acts of corruption during privatization in Czechoslovakia, and Bourke made statements during a conference call that showed concern with whether his agents were paying bribes.[128] All but the last of these factors would be red flags of doing business in a foreign country and should lead an organization to perform heightened due diligence before going forward.[129] Instead, the district court found that Bourke and his partners structured their enterprise to insulate themselves from further information about potential bribes.[130] By doing so, Bourke had "consciously avoided confirming" whether bribes would be paid, which was the last predicate for a conscious avoidance instruction.[131]

123. *Id*.
124. *Id*. at 374–78.
125. *Id*. at 385. The district court also explained that the government must offer "further proof that the defendant joined the conspiracy with the intent to further its criminal purpose." *Id*.
126. *Id*. at 385–86 (quoting United States v. Kaplan, 490 F.3d 110, 127 (2d Cir. 2007) (internal quotations omitted)).
127. *Id*. at 386.
128. *Id*. at 386–87.
129. *See id*. at 386–88.
130. *Id*.
131. *See id*. at 387–88. Bourke also argued that the district court had not charged the jury to find the he had acted "willfully" and "corruptly," which are the mens rea elements specified in the text of the FCPA. *See* FCPA § 104, 15 U.S.C. § 78dd-2(a) (2006). The district court rejected this argument, noting several instances where the jury instructions specifically asked jurors to make those findings. *Kozeny*, 664 F. Supp. 2d at 389–92.

Bourke also challenged his conviction on the ground that the district court had not submitted his requested jury charge on the defense that the payment was legal under Azeri law.[132] The FCPA provides a defense for a "payment, gift, offer, or promise of anything of value that was made, [that] was lawful under the written laws and regulations of the foreign official's . . . country."[133] The district court noted that the Azerbaijan Criminal Code proscribes bribery of government officials, and that it also provides that any "person who has given a bribe shall be *free* from criminal responsibility if with respect to him there was extortion of the bribe or if that person after giving the bribe voluntarily made a report of the occurrence."[134] The district court then interpreted the FCPA lawfulness defense to distinguish, on the one hand, payments that are lawful under a country's law, and on the other hand, payments that were illegal but where the bribe payer had a legal defense.[135] Because the text of the FCPA focuses on lawful "payments," the defense applied to the former but not the latter.[136] And because Azeri law made the payment illegal while giving the bribe payer a defense, Bourke was not entitled to a charge on the FCPA's lawfulness defense.[137]

The second major FCPA development was an Opinion Procedure Release from the United States Department of Justice ("DOJ") that provided guidance on sample products provided to potential government customers.[138] Release 09-01 concerned a private United States company that wanted to begin selling its medical devices to a foreign country's government.[139] The company already sold its devices to private companies in the country, and the government used devices made by the company's competitors.[140] The government planned to begin a new, subsidized program for the medical devices, but announced that it would endorse only those devices that it had reviewed and approved.[141] The foreign government requested that the company provide one hundred complementary devices and related accessories, with a value of about $1.9 million, for government review.[142] The number of devices was calculated based on the company providing ten

132. *Kozeny*, 664 F. Supp. 2d at 394.
133. FCPA § 104, 15 U.S.C. § 78dd-2(c)(1) (2006).
134. *Kozeny*, 664 F. Supp. 2d at 394.
135. *See id*. at 394–95.
136. *Id*.
137. *Id*.
138. FCPA Opinion Procedure Release No. 09-01 (Aug. 3, 2009), *available at* http://www.justice.gov/criminal/fraud/fcpa/opinion/2009/0901.pdf [hereinafter FCPA Opinion Procedure Release No. 09-01]. The FCPA charges the DOJ with responding to requests for guidance regarding application of the FCPA to specific transactions, *see* Foreign Corrupt Practices Act Amendments of 1988 § 5003(a), 15 U.S.C. §§ 78dd-1, 78dd-2 (2006), and the DOJ has promulgated rules governing such requests. *See* Foreign Corrupt Practices Act Opinion Procedure, 28 C.F.R. §§ 80.1–80.16 (2009). All other documents are collected on the DOJ's FCPA web page. *See Foreign Corrupt Practices Act Opinion Procedure Releases*, U.S. Dep't of Justice, http://www.justice.gov/criminal/fraud/fcpa/opinion/ (last visited June 20, 2010).
139. FCPA Opinion Procedure Release No. 09-01, *supra* note 138, at 1.
140. *Id*.
141. *Id*.
142. *Id*.

devices to each of ten different testing centers; the number of test centers was chosen to ensure an adequate sample size and thus valid test results.[143]

The company was apparently concerned that, under the FCPA, the DOJ might view the complementary medical devices as something of value given to influence the foreign government's decision whether to approve the company's devices. If a government official, or an official's family member, personally benefited from the free devices, there could be an FCPA violation.[144] Yet, the foreign government had a legitimate interest in testing medical devices before issuing approval.[145] The key was to design, implement, and document controls that ensured that the devices were actually used for valid testing purposes, and were not a personal benefit to a foreign government official.[146]

The company proposed several controls to prevent personal benefit due to the medical devices.[147] First, patients for the study were to be chosen based on objective criteria, and the selection process was to be open and transparent.[148] Second, the testing process itself was to be scientifically valid and transparent:

> The evaluation of the donated medical devices will be based on objective criteria that are standard for this type of medical device and that have been provided to the Department. The results of the evaluation will be collected by the Country Manager, who will enlist the help of two other medical experts to review the results and provide an overall report, as well as individual objective results, to a senior health official in the foreign country who will share his assessment with the Government Agency. The Government Agency will then evaluate the results of the evaluation and the report by the Country Manager, along with the senior health official's assessments, to determine the suitability of Requestor's technology for the medical device program. If the results of the evaluation are favorable, Requestor's device will be identified by the Government Agency as eligible for the subsidized medical device program, along with the devices of Requestor's competitors, which have already been declared eligible. The foreign government has advised the Requestor that none of the companies' devices will be promoted by the foreign government above any of the other qualified devices.[149]

Third, the test results would be provided to about thirty different test centers around the country, and those centers, not the central government official requesting the devices, would make decisions whether to purchase the devices.[150] Fourth, the company knew of no information or red flags to suggest that the foreign government official requesting the devices would personally benefit from the complementary items.[151]

143. *Id.*
144. *See* 15 U.S.C. §§ 78dd-1, 78dd-2 (2006).
145. *See* FCPA Opinion Procedure Release No. 09-01, *supra* note 138, at 1–2.
146. *See id.* at 2.
147. *Id.*
148. *Id.*
149. *Id.* at 2–3.
150. *Id.* at 3.
151. *Id.*

If the company successfully implemented the described controls, the DOJ opined that it would not take enforcement action against the company:

> [B]ased on Requestor's representations, the proposed provision of 100 medical devices and related items and services fall outside the scope of the FCPA in that the donated products will be provided to the foreign government, as opposed to individual government officials, for ultimate use by patient recipients selected in accordance with specific guidelines, as described above.[152]

The DOJ's opinion is quite sensible—the company took strong measures to ensure that the foreign government would actually use the devices for the asserted purpose. The DOJ cannot reasonably ask more of a company planning to do business abroad, and consequently the controls set forth in this release should serve as a starting point for any firm asked to provide sample products or services for evaluation by a foreign government. That said, the company still faces challenges going forward. At a minimum, the company must adequately implement, monitor, and document these controls. In addition, the company should be prepared to respond to any information or indication that the complementary devices are being diverted to improper uses. An effective compliance and ethics program should be equipped to provide these safeguards.

2. Organisation for Economic Cooperation and Development ("OECD") Compliance Guidance

About twenty years after the United States became the first country to ban bribery of foreign government officials, OECD countries signed the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. The Convention went into effect in February 1999, and requires participating nations, of which there are now thirty-eight, to ensure that their domestic law contains specified legal prohibitions on the bribery of foreign government officials.[153] The OECD tracks and reports on legal developments within participating nations, as well as on enforcement of those laws. The United States deposited its instrument of ratification on December 8, 1999, and shortly thereafter amended provisions of the FCPA to conform to provisions of the Convention.[154]

To further encourage anti-bribery efforts, the OECD Council adopted the Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions on November 26, 2009.[155] One

152. *Id.*

153. *See* Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, Dec. 8, 1998, 112 Stat. 1302, 37 I.L.M. 1.

154. For example, the FCPA was amended to extend its coverage to any person who takes any action in furtherance of a bribe while within the territory of the United States, regardless of whether that person is a citizen or resident of the United States. *See* International Anti-Bribery and Fair Competition Act of 1998, Pub. L. No. 105-366, 112 Stat. 3302 (1998) (codified at 15 U.S.C. §§ 78dd-1–78dd-3, 78ff (2006)).

155. OECD Working Grp. on Bribery in Int'l Bus. Transactions, Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions (Nov. 26, 2009), *available at* http://www.oecd.org/dataoecd/11/40/44176910.pdf [hereinafter OECD Recommendation].

provision of this document emphatically endorses domestic laws that encourage organizations to adopt anti-bribery compliance and ethics programs: "Member countries should encourage . . . companies to develop and adopt adequate internal controls, ethics and compliance programmes or measures for the purpose of preventing and detecting foreign bribery, taking into account the Good Practice Guidance on Internal Controls, Ethics, and Compliance . . . ."[156] Three months later, on February 18, 2010, the OECD Council adopted the Good Practice Guidance on Internal Controls, Ethics, and Compliance as a supplement to the Recommendation of November 2009.[157] This document outlined the basic framework for an effective anti-bribery compliance and ethics program. The framework parallels the organizational sentencing Guidelines and other similar standards, placing them in the context of bribery of foreign government officials. For example, one provision encourages adoption of:

> [E]thics and compliance programmes or measures designed to prevent and detect foreign bribery, applicable to all directors, officers, and employees, and applicable to all entities over which a company has effective control, including subsidiaries, on, *inter alia*, the following areas:
>
> i) gifts;
> ii) hospitality, entertainment and expenses;
> iii) customer travel;
> iv) political contributions;
> v) charitable donations and sponsorships;
> vi) facilitation payments; and
> vii) solicitation and extortion . . . .[158]

This listing jump-starts the organization's risk assessment, identifying various items that raise risks of foreign bribery. Also, the OECD Guidance follows the proposed amendments to the federal sentencing Guidelines, discussed above, in recommending that the compliance officer have authority to report directly to the organization's board:

> [O]versight of ethics and compliance programmes or measures regarding foreign bribery, including the authority to report matters directly to independent monitoring bodies such as internal audit committees of boards of directors or of supervisory boards, is the duty of one or more senior corporate officers, with an adequate level of autonomy from management, resources, and authority.[159]

Of note, the OECD Recommendation and Guidance directs signatory nations, including the United States, to take measures to "encourage" organizations to design, implement, and operate anti-bribery ethics and compliance programs.[160] Currently, the United States has no incentives targeted at encouraging such anti-

156. *Id.* § X.C.(i).
157. *Id.*
158. *Id.* annex II (A.5).
159. *Id.* annex II (A.4).
160. *Id.* § X.

bribery programs. Rather, domestic law provides only generic incentives for overall compliance and ethics programs, such as the possibility of prosecutorial leniency under the Filip Memorandum and the sentencing credit under the organizational sentencing Guidelines.[161] As discussed in the next section, the United Kingdom now outpaces the United States in this area by providing organizations an affirmative defense for an effective anti-bribery compliance and ethics program.

3. United Kingdom Bribery Act

The United Kingdom adopted the Bribery Act 2010 this past April,[162] consolidating its laws on bribery and corruption. One section of that law defines a specific criminal offense of bribery of a foreign government official.[163] That part of the new law holds significance for compliance professionals for two reasons. First, the law's scope is slightly different from the FCPA, meaning that organizations subject to both the FCPA and the Bribery Act must adjust their anti-bribery ethics and compliance programs accordingly. Second, unlike the FCPA, the Bribery Act provides an affirmative defense for firms with an effective compliance and ethics program.[164] This section addresses each aspect of the new law in turn.

The Bribery Act's basic offense for bribery of a foreign government official parallels the FCPA in many respects. For example, both laws apply to offers and promises as well as actual payments, cover non-monetary bribes as well as money, and allow payments that are legal under the written law of a foreign country.[165] The Bribery Act, however, is broader than the FCPA in one important respect: while the FCPA permits facilitating or "grease" payments, the Bribery Act makes no such exception.[166] Facilitating payments are relatively small amounts paid to obtain a routine government function or service—such as mail delivery—that an organization is entitled to under foreign law.[167] This difference between the FCPA and the Bribery Act will be important to United States corporations because the Bribery Act specifically applies to "any . . . body corporate (wherever incorporated) which carries on a business, or part of a business, in any part of the United Kingdom."[168] Consequently, a United States corporation that does business in the United Kingdom must adjust its anti-bribery compliance and ethics program to take account of the more stringent provisions of the Bribery Act.

The Bribery Act offers a powerful incentive for covered organizations to adopt an anti-bribery compliance and ethics program. The law provides that "it is a

161. For a discussion of the incentives under the Filip memorandum, see *Survey V*, *supra* note 1, at 197–200.

162. *See* Bribery Act, 2010, c. 23 (Eng.).

163. *Id.* § 6.

164. *See id.* § 7(2).

165. *See id.* § 6; FCPA § 104, 15 U.S.C. § 78dd-2 (2006).

166. *Compare* 15 U.S.C. § 78dd-2(b), *with* Bribery Act § 6.

167. 15 U.S.C. § 78dd-2(b) (The FCPA "shall not apply to any facilitating or expediting payment to a foreign official, political party, or party official the purpose of which is to expedite or to secure the performance of a routine governmental action by a foreign official, political party, or party official.").

168. Bribery Act § 7(5)(b) (defining a "relevant commercial organisation").

defence for [an organization] to prove that [the organization] had in place adequate procedures designed to prevent persons associated with [the organization] from undertaking such conduct."[169] The law then directs the Secretary of State to "publish guidance about procedures that relevant commercial organisations can put in place to prevent persons associated with them from bribing,"[170] and that the Secretary of State "may, from time to time, publish revisions to guidance under this section or revised guidance."[171] Notably, the law's text does not provide *any* factors or other indications of what such a program would entail. That said, one should not be surprised if the resulting guidelines closely track the OECD compliance best practices guidance discussed in the preceding section. After all, the United Kingdom is a signatory to the OECD Convention, and the OECD has previously criticized the United Kingdom for lax enforcement of its anti-bribery laws.[172] Regardless of its form, however, the very fact that the Bribery Act offers a full defense to criminal wrongdoing likely ensures that the Secretary's guidance, when released, will receive wide consideration by compliance professionals around the globe.

B. European Data Privacy Laws

Reporting hotlines have long been mainstays of corporate compliance and ethics programs in the United States. The original federal organizational sentencing Guidelines listed a reporting line as one of its seven steps,[173] the Sarbanes-Oxley Act of 2002 requires public companies to have a "confidential, anonymous" reporting procedure for financial misconduct,[174] and regulatory compliance standards covering a wide array of areas, including health care[175] and federal contracting,[176] all incorporate a reporting line as an essential component. And all of these standards counsel organizations either to allow or encourage anonymous reporting of misconduct, along with a strict requirement of non-retaliation.[177] The philosophy seems to be that anonymity promotes candor, and that the lessons of recent scan-

169. *Id.* § 7(2).
170. *Id.* § 9(1).
171. *Id.* § 9(2).
172. OECD Working Grp. on Bribery in Int'l Bus. Transactions, United Kingdom: Phase 2bis—Report on the Application of the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and the 1997 Recommendation on Combating Bribery in International Business Transactions 4 (Oct. 16, 2008), *available at* http://www.oecd.org/dataoecd/23/20/41515077.pdf. ("The Working Group is particularly concerned that the UK's continued failure to address deficiencies in its laws on bribery of foreign public officials and on corporate liability for foreign bribery has hindered investigations.").
173. *See* USSG § 8B2.1(b)(5)(C) (2009) ("The organization shall take reasonable steps . . . to 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.").
174. Sarbanes-Oxley Act of 2002 § 301, 15 U.S.C. § 78j-1(m)(4)(B) (2006).
175. *See, e.g.*, Publication of the OIG Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8987 (Feb. 23, 1998).
176. *See* 48 C.F.R. § 52.203-13(c)(2)(ii)(D) (2009).
177. *See supra* notes 173–76 and accompanying text.

dals is that honest employees need the cover of anonymity to overcome the social pressure inherent in an unethical corporate culture.

As United States companies have tried to export their hotlines to the EU, they have met legal obstacles. This conflict arises from an EU legal framework that grows from different cultural roots. While the United States has embraced whistleblower hotlines as an effective means to detect corporate wrongdoing, EU countries view such reporting with deep suspicion born of experiences in World War II.[178] Many European countries live in the shadow of an era where people turned in their fellow citizens to the Nazi government to gain favor.[179] Against this background, reporting lines are possible tools of harassment, and anonymous reporting makes such abuses easier. For example, one document promulgated by a French government authority recites that "[t]he possibility to file anonymous reports can only increase the risk of slanderous reports."[180]

The EU's cultural assumptions are apparent in the comprehensive legal framework governing data privacy. While the United States leaves data privacy protection to a disjointed hodgepodge of legal rules at the federal, state, and local level, the EU has enshrined the right in its Fundamental Charter:

> ARTICLE 8
>
> Protection of personal data
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.[181]

United States citizens must depend on the good graces of government to enact data protection laws, while EU citizens have a comprehensive constitution-like

178. *See* Donald C. Dowling, Jr., *Sarbanes-Oxley Whistleblower Hotlines Across Europe: Directions Through the Maze*, 42 Int'l Law. 1, 12 (2008); Letter from Peter Schaar, Chairman, EU Article 29 Data Prot. Working Party, to Ethiopis Tafara, Dir., U.S. Sec. & Exch. Comm'n Office of Int'l Affairs 3 (July 3, 2006), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2006-07-03-reply_whistleblowing.pdf ("[A]nonymous reporting evokes some of the darkest times of recent history on the European continent, whether during World War II or during more recent dictatorships in Southern and Eastern Europe. This historical specificity makes up for a lot of the reluctance of EU Data Protection Authorities to allow anonymous schemes being advertised as such in companies as a normal mode of reporting concerns.").

179. *See* Dowling, *supra* note 178, at 12.

180. Commission nationale de l'informatique et des libertés, Guideline Document Adopted by the "Commission nationale de l'informatique et des libertés" (CNIL) on 10 November 2005 for the Implementation of Whistleblowing Systems in Compliance with the French Data Protection Act of 6 January 1978, as Amended in August 2004, Relating to Information Technology, Data Filing Systems and Liberties 4 (Nov. 10, 2005), *available at* http://www.cnil.fr/fileadmin/documents/en/CNIL-recommandations-whistleblowing-VA.pdf [hereinafter CNIL Guideline Document].

181. Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 10, *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

right to such protection. Further, the EU mandate is to be administered by independent data protection agencies in each member country.[182] To assist the national data protection agencies, an EU directive has created a Working Party that promulgates guidelines for ensuring data protection.[183] The group is known as the Article 29 Working Party, as it was created by Article 29 of the EU directive on data protection.[184]

The reporting hotlines required by some United States laws raise concerns squarely within the scope of the EU's data protection right.[185] This conflict first came to a head in 2005 when McDonald's Corporation sought to implement its Sarbanes-Oxley financial reporting hotline in France.[186] French authorities initially denied permission, putting McDonald's between a rock and a hard place.[187] In short, the only way to comply with both United States and EU law would have been for McDonald's to cease operations in France. Later that year, the French data privacy authority adopted a narrow allowance for reporting hotlines.[188] For example, the French regulations prohibit an organization from encouraging anonymous reporting;[189] require timely destruction of the data collected;[190] and strictly limit the scope of such hotlines to accounting, audit, and bribery, "unless the vital interest of the company or the physical or moral integrity of its employees are at stake."[191]

In 2006, the Article 29 Working Party released guidance on how EU member nations might ensure data privacy protection in the operation of hotlines.[192] Among other aspects, the Working Party guidance document specifically paralleled the French agency's stance on anonymous reporting:

> The Working Party considers that whistleblowing schemes should be built in such a way that they do not encourage anonymous reporting as the usual way to make a complaint. In particular, companies should not advertise the fact that anonymous

182. *Id.* art. 8(3).

183. *See* Council Directive 95/46/EC of the European Parliament of October 24, 1995, 1995 O.J. (L 281) 31, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

184. *Id.* art. 29.

185. Even if a hotline complies with EU regulations, an American company will also face data protection issues if it tries to transfer hotline information outside of the EU. *See* Brett Tarr, *The Nuts & Bolts of the EU Safe Harbor*, Ass'n Corp. Couns. Docket, Nov. 2009, at 106, 108.

186. *See* Dowling, *supra* note 178, at 20–21.

187. *See id.*

188. CNIL Guideline Document, *supra* note 180, at 2.

189. *Id.* at 5 ("[T]he organisation must not encourage the persons who are to use the system to do so anonymously, and the publicity which is made on the existence of such a system must be designed by taking this requirement into account. On the contrary, the procedure must be designed in such a way that the employees using the system are requested to identify themselves each time they make an alert and report information relating to facts rather than to individuals.").

190. *Id.* at 6 ("Data relating to alerts giving rise to an investigation must not be stored beyond two months from the close of verification operations, unless a disciplinary procedure or legal proceedings are initiated against the person incriminated in the report or the author of an abusive alert.").

191. *Id.* at 3.

192. Article 29 Data Prot. Working Party, Opinion 1/2006 on the Application of EU Data Protection Rules to Internal Whistleblowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking and Financial Crime (Feb. 1, 2006), *available at* http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2006_en.htm.

> reports may be made through the scheme. On the contrary, since whistleblowing schemes should ensure that the identity of the whistleblower is processed under conditions of confidentiality, an individual who intends to report to a whistleblowing system should be aware that he/she will not suffer due to his/her action. For that reason a scheme should inform the whistleblower, at the time of establishing the first contact with the scheme, that his/her identity will be kept confidential at all the stages of the process and in particular will not be disclosed to third parties, either to the incriminated person or to the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. It is also necessary to make whistleblowers aware that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of the enquiry conducted by the whistleblowing scheme.[193]

The Working Party, then, discourages anonymous reporting partly out of suspicion, and partly out of doubt concerning its necessity. First, anonymous reporting increases the likelihood of abuses by eliminating accountability for false or harassing reports. Second, if a hotline is properly designed and operated to ensure confidentiality, then a person making a report need not fear retaliation, and anonymity is unnecessary. So, anonymous reporting is a dangerous tool that is not needed. The Working Party grudgingly allowed such reporting as a concession to reality—anonymous reports will happen, and organizations should not be forced simply to ignore them. But organizations should not use that reality as an excuse to encourage or endorse such reports.

The Spanish Data Protection Agency has gone one step further, providing nonbinding guidance that organizations should not accept anonymous reports.[194] While the Working Party bowed to reality, the Spanish authority concluded that a strict promise of confidentiality left no need for anonymous reporting.[195] And in October 2009, the Portuguese data protection agency reached the same conclusion, issuing guidance that bans anonymous reporting.[196] Given the differing positions among EU member nations on anonymity, an organization doing business throughout the EU must either bar anonymous reports, have separate hotlines for different countries, or train hotline personnel to screen calls based on their point of origin. In other words, a United States company cannot unthinkingly export its Sarbanes-Oxley hotline to the EU.

---

193. *Id.* at 11.

194. *See* Dowling, *supra* note 178, at 38. The Spanish guidance was issued in response to the request of a private organization for an opinion concerning the legality of a proposed hotline. *Id.* For an additional summary of how member nations have implemented the data privacy requirements as applied to hotlines, see Steve Lauer & Nick Ciancio, *Setting Up an Ethics and Compliance Hotline/Helpline*, *in* 1 Corporate Compliance Practice Guide: The Next Generation of Compliance 9-1 (C. Basri ed., 2009).

195. *See* Dowling, *supra* note 178, at 38.

196. DELIBERAÇÃO Nº 765/2009 (in the original Portuguese), *available at* http://www.cnpd.pt/bin/orientacoes/DEL765-2009_LINHAS_ETICA.pdf. The author has not found an English translation of the regulations, and so the text relies on secondary sources. *See* Doug Cornelius, *Portugal and Ethics Hotlines*, Compliance Building (June 2, 2010, 8:00 AM), http://www.compliancebuilding.com/2010/06/02/portugal-and-ethics-hotlines/.

Appendix A

New York Social Services Law § 363-d Provider Compliance Program

1. The legislature finds that medical assistance providers may be able to detect and correct payment and billing mistakes and fraud if required to develop and implement compliance programs. It is the purpose of such programs to organize provider resources to resolve payment discrepancies and detect inaccurate billings, among other things, as quickly and efficiently as possible, and to impose systemic checks and balances to prevent future recurrences. The legislature accordingly declares that it is in the public interest that providers within the medical assistance program implement compliance programs. The legislature also recognizes the wide variety of provider types in the medical assistance program and the need for compliance programs that reflect a provider's size, complexity, resources, and culture. For a compliance program to be effective, it must be designed to be compatible with the provider's characteristics. At the same time, however, the legislature determines that there are key components that must be included in every compliance program and such components should be required if a provider is to be a medical assistance program participant. Accordingly, the provisions of this section require providers to adopt effective compliance program elements, and make each provider responsible for implementing such a program appropriate to its characteristics.

2. Every provider of medical assistance program items and services that is subject to subdivision four of this section shall adopt and implement a compliance program. The office of Medicaid inspector general shall create and make available on its website guidelines, which may include a model compliance program, that reflect the requirements of this section. Such program shall at a minimum be applicable to billings to and payments from the medical assistance program but need not be confined to such matters. The compliance program required pursuant to this section may be a component of more comprehensive compliance activities by the medical assistance provider so long as the requirements of this section are met. A compliance program shall include the following elements:

   (a) written policies and procedures that describe compliance expectations as embodied in a code of conduct or code of ethics, implement the operation of the compliance program, provide guidance to employees and others on dealing with potential compliance issues, identify how to communicate compliance issues to appropriate compliance personnel and describe how potential compliance problems are investigated and resolved;
   (b) designate an employee vested with responsibility for the day-to-day operation of the compliance program; such employee's duties may

solely relate to compliance or may be combined with other duties so long as compliance responsibilities are satisfactorily carried out; such employee shall report directly to the entity's chief executive or other senior administrator and shall periodically report directly to the governing body on the activities of the compliance program;

(c) training and education of all affected employees and persons associated with the provider, including executives and governing body members, on compliance issues, expectations and the compliance program operation; such training shall occur periodically and shall be made a part of the orientation for a new employee, appointee or associate, executive and governing body member;

(d) communication lines to the responsible compliance position, as described in paragraph (b) of this subdivision, that are accessible to all employees, persons associated with the provider, executives and governing body members, to allow compliance issues to be reported; such communication lines shall include a method for anonymous and confidential good faith reporting of potential compliance issues as they are identified;

(e) disciplinary policies to encourage good faith participation in the compliance program by all affected individuals, including policies that articulate expectations for reporting compliance issues and assist in their resolution and outline sanctions for: (1) failing to report suspected problems; (2) participating in non-compliant behavior; or (3) encouraging, directing, facilitating or permitting non-compliant behavior; such disciplinary policies shall be fairly and firmly enforced;

(f) a system for routine identification of compliance risk areas specific to the provider type, for self-evaluation of such risk areas, including internal audits and as appropriate external audits, and for evaluation of potential or actual non-compliance as a result of such self-evaluations and audits;

(g) a system for responding to compliance issues as they are raised; for investigating potential compliance problems; responding to compliance problems as identified in the course of self-evaluations and audits; correcting such problems promptly and thoroughly and implementing procedures, policies and systems as necessary to reduce the potential for recurrence; identifying and reporting compliance issues to the department or the office of Medicaid inspector general; and refunding overpayments;

(h) a policy of non-intimidation and non-retaliation for good faith participation in the compliance program, including but not limited to reporting potential issues, investigating issues, self-evaluations, audits and remedial actions, and reporting to appropriate officials as provided in sections seven hundred forty and seven hundred forty-one of the labor law.

3. Upon enrollment in the medical assistance program, a provider shall certify to the department that the provider satisfactorily meets the requirements of this section. Additionally, the commissioner of health and Medicaid inspector general shall have the authority to determine at any time if a provider has a compliance program that satisfactorily meets the requirements of this section.

   (a) A compliance program that is accepted by the federal department of health and human services office of inspector general and remains in compliance with the standards promulgated by such office shall be deemed in compliance with the provisions of this section, so long as such plans adequately address medical assistance program risk areas and compliance issues.
   (b) In the event that the commissioner of health or the Medicaid inspector general finds that the provider does not have a satisfactory program within ninety days after the effective date of the regulations issued pursuant to subdivision four of this section, the provider may be subject to any sanctions or penalties permitted by federal or state laws and regulations, including revocation of the provider's agreement to participate in the medical assistance program.

4. The Medicaid inspector general, in consultation with the department of health, shall promulgate regulations establishing those providers that shall be subject to the provisions of this section including, but not limited to, those subject to the provisions of articles twenty-eight and thirty-six of the public health law, articles sixteen and thirty-one of the mental hygiene law, and other providers of care, services and supplies under the medical assistance program for which the medical assistance program is a substantial portion of their business operations.