A New Day for Healthcare Organizations: Sarbanes-Oxley Certification Requirements, Compliance, and Exposures

Ronald H. Levine, Esquire
Post & Schell PC
Philadelphia, Pennsylvania*

Jennifer A. Short, Esquire
Holland & Knight LLP
McLean, Virginia†

* Ronald H. Levine, Esq. (rlevine@postschell.com) is a partner at the Philadelphia-based law firm of Post & Schell, P.C., heading its White Collar Defense, Corporate Compliance and Risk Management practice group. Mr. Levine was previously the chief of the Criminal Division of the U.S. Attorney’s Office for the Eastern District of Pennsylvania.

† Jennifer A. Short, Esq. (jennifer.short@hklaw.com) is a partner in the McLean, Virginia office of the law firm Holland & Knight LLP, where she specializes in healthcare fraud defense, corporate compliance, and complex commercial litigation.

† This White Paper is issued by the Sarbanes-Oxley Act Task Force. The Task Force is sponsored by the HMOs and Health Plans, Tax and Finance, and Hospitals and Health Systems Practice Groups of the American Health Lawyers Association. The Task Force co-chairs, and the co-editors of this White Paper, are Stuart I. Silverman, Esq. (Office of the Inspector General for the District of Columbia) and Douglas K. Anning, Esq. (Seigfreid Bingham Levy Selzer & Gee PC). DISCLAIMER: Any views and opinions expressed by Stuart Silverman, as co-editor of the White Paper, cannot be attributed to, and do not represent, the position of the Office of the Inspector General for the District of Columbia.

The Sarbanes-Oxley Act Task Force wishes to acknowledge members of its Advisory Council for their contributions as reviewers of this paper. They are:

Bruce A. Baird, Esq.
Covington & Burling
Washington, DC

Professor Dennis Beresford
University of Georgia
Athens, GA.

Professor Jennifer Bethel
Babson College
Wellesley, MA

Professor James D. Cox
Duke University Law School
Durham, NC

Judge Stanley Sporkin
Weil, Gotshal & Manges
Washington, DC

Thomas W. White, Esq.
Wilmer Cutler & Pickering
Tysons Corner, VA
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>A. The Healthcare Backdrop to the SOA</td>
<td>3</td>
</tr>
<tr>
<td>B. Post-SOA Healthcare Prosecutions: United Memorial, Alvarado, and HealthSouth</td>
<td>4</td>
</tr>
<tr>
<td>II. PRE-SOA DISCLOSURE LAW AND RELATED CRIMINAL STATUTES</td>
<td>7</td>
</tr>
<tr>
<td>A. SEC Filing-Related Statutes and Regulations</td>
<td>7</td>
</tr>
<tr>
<td>B. General Securities Fraud</td>
<td>8</td>
</tr>
<tr>
<td>1. The Pre-SOA Securities Fraud Statutes</td>
<td>8</td>
</tr>
<tr>
<td>2. The SOA Securities Fraud Statute</td>
<td>9</td>
</tr>
<tr>
<td>C. False Statements, Mail and Wire Fraud</td>
<td>11</td>
</tr>
<tr>
<td>D. Healthcare Fraud</td>
<td>12</td>
</tr>
<tr>
<td>E. Tax Exempt Bond-Related Disclosure Fraud</td>
<td>13</td>
</tr>
<tr>
<td>III. SARBANES-OXLEY DISCLOSURE: THE “CIVIL” § 302</td>
<td>15</td>
</tr>
<tr>
<td>A. Statutory Overview of § 302</td>
<td>15</td>
</tr>
<tr>
<td>B. Regulatory Overview of § 302</td>
<td>17</td>
</tr>
<tr>
<td>1. Content of Certification</td>
<td>18</td>
</tr>
<tr>
<td>2. Form and Location of Certification</td>
<td>20</td>
</tr>
<tr>
<td>C. Comparing the § 302 Certification to Other Routine Certifications in the Healthcare Industry</td>
<td>20</td>
</tr>
<tr>
<td>IV. SARBANES-OXLEY DISCLOSURE: THE “CRIMINAL” § 906</td>
<td>23</td>
</tr>
<tr>
<td>A. Statutory Overview of § 906</td>
<td>23</td>
</tr>
<tr>
<td>B. Analysis of Criminal Liability Under SOA § 906</td>
<td>25</td>
</tr>
</tbody>
</table>
1. State of Mind ................................................................. 25
2. Defenses ................................................................. 26
3. Criminal Penalties .................................................... 29

V. IMPACT OF SOA ON ORGANIZATIONS ........................................ 33
   A. Prosecuting Organizations ....................................... 33
   B. Sentencing Organizations ........................................ 34
   C. Impact on Privately Held and Not-For-Profit
      Healthcare Organizations ........................................ 36

VI. COMPLIANCE IMPLICATIONS .................................................... 38
   A. SOA Mandates Internal Controls Over “Disclosure”
      and “Financial Reporting” ........................................ 38
   B. The Challenge for Privately Held and
      Not-For-Profit Organizations .................................... 39
   C. Creating an Effective Compliance Program ..................... 40
      1. What are the Company’s Potential Areas of Risk? ....... 42
      2. How can the Company Disseminate Information
         to Those who Need it? ....................................... 43
      3. What Mechanisms are in Place to Ensure That
         Information is Being Reported to Those who
         Need to Know and can React to it? ....................... 43
      4. Does the Company Have Policies and Procedures
         in Place to Address Problems That may Arise, and
         is Action in Fact Taken When an Issue is Discovered? .... 45
      5. Has Company Management Emphasized Compliance
         in Such a Manner as to Infuse the Corporate
         Culture With a Sense That Ethical Behavior Is
         Rewarded? ............................................................. 46

VII. CONCLUSION ....................................................................... 47
I. INTRODUCTION

Since 2001, the United States has witnessed a series of events that have provoked a legislative and regulatory response likely to change the face of corporate governance for all companies, including healthcare organizations, whether or not they are publicly traded or for-profit. The September 2001 terrorist attacks on the World Trade Center—a symbol of America's financial strength—were followed closely by a series of corporate scandals and bankruptcies that shook public confidence in U.S. markets. The spectacular collapse of Enron Corporation, the indictment of Arthur Andersen, LLP, and the collateral damage sustained by employees and investors of these and other companies that engaged in "creative accounting" all contributed to a political climate in 2002 in which Congress sought to crack down on corporate abuses and reassure the investing public.¹

These events have brought to a crescendo a theme the early notes of which were sounded in the 1996 milestone opinion of In re Caremark International, Inc.² A very hot spotlight is now focused on the obligation of corporate management and the board of directors to ensure the integrity of information reporting systems within the corporation and on management’s certification to the outside world of the accuracy of that information.

On July 30, 2002, in the wake of these corporate financial and accounting fraud scandals, President Bush signed the Sarbanes-Oxley Act (SOA).³ Ostensibly, the SOA is aimed at publicly owned corporations and imposes substantial obligations on those companies to disclose and certify to the true and accurate financial condition of their businesses, while subjecting them to unprecedented scrutiny from government regulators and oversight boards. While some industry groups—healthcare providers and insurers, for example—are accustomed to detailed and sometimes confusing government rules and procedures, many businesses are facing government supervision and examination at a level more intense than they may have experienced in the past.

One of the primary goals of the SOA is to increase the financial transparency and accountability of publicly traded companies. The SOA contains numerous provisions that empower the Securities and Exchange Commission (SEC) to make and enforce rules in accordance with the purpose and intent of the Act. In the year following passage of the SOA, the SEC issued thirteen proposed rulemakings and adopted eleven final rulemakings related to Sarbanes-Oxley.⁴

² 698 A.2d 959 (Del. Ch. 1996) (Board has duty to assure, for compliance purposes, that adequate corporate information gathering and reporting systems exist.).
While many provisions of the SOA, including its financial certification provisions, specifically apply to public corporations (including, of course, publicly traded healthcare providers, pharmaceutical manufacturers, managed care organizations, and the like), some provisions of the SOA also apply directly to privately owned entities, including not-for-profit healthcare corporations. These include new SOA criminal provisions concerning obstruction of justice via document destruction and retaliation against whistleblowers. Regarding registered public accounting firms, SOA provisions include new conflict of interest restrictions and oblige the SEC to promulgate standards for auditing an organization’s internal financial controls. These same accounting firms also frequently audit or perform work for non-publicly traded organizations in the healthcare sector, so that the regulations governing them will impact private companies, albeit indirectly.

For the reasons discussed in this white paper, we also think that other governance provisions of the SOA inevitably will be applied de facto, due to market pressures, or de jure, due to enhanced state regulation, outside the sphere of publicly traded corporations, i.e., to not-for-profit healthcare institutions. These include new SOA provisions, civil and criminal, requiring CEOs and CFOs to certify to the accuracy of their institution’s financial statements and reports and to the adequacy of its information reporting systems. It is these SOA certification requirements that this white paper addresses.

---

5 18 U.S.C. §§ 1519 (SOA § 802), 1512. Healthcare counsel should note that these SOA provisions significantly expand the government’s ability to charge obstruction of justice for actions committed after July 30, 2002. Most importantly, the broad wording of § 1519 does not appear to require that a federal investigation actually be pending, known about, or even expected at the time of the alleged obstruction. Rather, the knowing destruction or alteration of documents “in contemplation of” the “proper administration of any matter” before “any” federal agency can constitute obstruction. Id. at § 1519. Of course, the “administration of a matter” before a federal agency can occur long before a civil or criminal investigation commences.


8 15 U.S.C. § 7262 (SOA § 404); see “An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements,” PCAOB Release No. 2003-017 (Oct. 7, 2003), available at: http://www.pcaobus.org/pcaob_rulemaking.asp. The Public Company Accounting Oversight Board (PCAOB) is an SEC-supervised, non-profit corporation created by the SOA to oversee the auditors of public companies. SOA §§ 404 and 103 direct the PCAOB to establish professional standards governing the independent auditor’s attestation to, and reporting on, management’s assessment of the effectiveness of internal controls. On October 7, 2003, the PCAOB issued for public comment this audit standard, which addresses the work that is required to audit internal control over financial reporting and the relationship of that audit to the audit of the financial statements.


A. The Healthcare Backdrop to the SOA

There is no doubt that healthcare companies are within the sights of this renewed focus on corporate governance. Indeed, the healthcare industry—perhaps precisely because it is and has been a heavily regulated industry—has a long and storied role in the corporate governance debate.

Healthcare counsel might recall that the Caremark case, as well two subsequent major accounting scandals, actually arose in the healthcare sector between 1995 and 2000. This was well before Enron et al. were even a gleam in the eye of the federal government’s SOA-inspired Corporate Fraud Task Force.\(^{11}\)

In the 1990s, Caremark International, Inc. provided alternative site healthcare services (e.g., home infusion) and operated a managed-care prescription drug program. In 1994, Caremark was indicted on charges of violating the Medicare Anti-Kickback Statute. The company eventually pleaded guilty to a single count of mail fraud. The well-known Caremark case arose out of a motion to the Court of Chancery of Delaware to approve a settlement of a parallel shareholder derivative suit involving claims that Caremark’s board of directors had breached its fiduciary duty to the corporation.

In assessing and ultimately approving the proposed settlement, the court reasoned that in theory a board could be held liable for a failure to monitor. Specifically, the court found that a corporate board must exercise good faith judgment and assure itself that “the corporation’s information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility.”\(^{12}\)

Thus the concept of adequate internal control and reporting systems, and the board’s responsibilities in that regard, were highlighted by the Caremark case. The opinion has had a broad influence on corporate board governance both within and outside the healthcare sector.

Two subsequent accounting scandals in the healthcare sector concerned the collapse of the not-for-profit Allegheny Health, Education and Research Foundation (AHERF) hospital system, and the mammoth earnings restatements of the publicly traded Rite Aid Corporation. In essence, prosecutions in each of these cases related back to allegedly false and fraudulent financial statements.

In 1997, AHERF was the largest not-for-profit healthcare organization in Pennsylvania. In July of 1998, AHERF filed for bankruptcy protection with over $1 billion in liabilities. Allegations of misrepresentations of income in financial statements and in disclosure statements.

---

\(^{11}\) The Corporate Fraud Task Force was created by Executive Order #13271 on July 9, 2002. It combines the efforts of the Departments of Justice and Treasury, the SEC, and other agencies, and takes credit for over 250 corporate fraud convictions, including those of at least 25 former CEOs. Task Force achievements are available at: http://www.usdoj.gov/dag/cftf/cases.html.

reports to the Municipal Securities Information Repositories (MSIRs) quickly surfaced.\textsuperscript{13} In April of 2000, AHERF’s CEO was prosecuted criminally by the Pennsylvania Attorney General, pleaded no contest to the charge of misappropriating entrusted property, and was sentenced to 11½ to 23 months in prison.\textsuperscript{14} A month later, without admissions of liability, AHERF’s CFO and other senior AHERF officials settled civil fraud allegations with the SEC regarding AHERF’s financial statements and disclosures to MSIRs.\textsuperscript{15}

Similarly, in the summer of 2000, Pennsylvania-based Rite Aid Corporation, a large retail pharmacy chain, restated its earnings by $1.6 billion, then the largest earnings restatement in United States history (later topped by WorldCom and others). Ensuing federal prosecutions of Rite Aid senior management related to, among other things, allegedly fraudulent disclosures to the SEC and obstruction of justice.\textsuperscript{16} This investigation has resulted in the convictions of Rite Aid’s former CEO, CFO, CLO, and other managers. They await sentencing.

\begin{itemize}
\item \textbf{B. Post-SOA Healthcare Prosecutions: \textit{United Memorial, Alvarado, and HealthSouth}}
\end{itemize}

Three federal criminal investigations after the SOA’s enactment have made crystal clear that healthcare institutions—and the individuals that run them—are within the sphere of corporate governance concerns and will not be immune from criminal prosecution.

In January of 2003, the not-for-profit United Memorial Hospital in Michigan signed a federal guilty plea agreement in which it admitted to fraud in connection with the alleged over utilization of pain management surgical procedures, one of which resulted in the death of a patient. Sentencing has been deferred, and it is possible that United Memorial’s guilty plea will be expunged in the future.\textsuperscript{17} However, a careful reading of the allegations contained in United Memorial’s plea agreement\textsuperscript{18} reads like a primer on corporate governance “not-tos” from the board on down. The hospital’s systems for information reporting, internal audit and investigation, conflict of interest disclosure, and responding to complaints all were questioned.

\begin{itemize}
\item \textsuperscript{15} See SEC v. McConnell and Morrison, CA No. 00-CV-2261 (E.D. Pa., May 2, 2000); In re Adamczak, CPA, Exchange Act Release No. 42743 (May 2, 2000); In re Spargo, CPA, Exchange Act Release No. 42742 (May 2, 2000).
\item \textsuperscript{16} United States v. Grass, Bergonzi, Brown, Sorkin, 1:Cr-02-146-01 (W.D. Pa., June 21, 2002).
\item \textsuperscript{17} A $1.05 million fine levied on United Memorial, however, will not be expunged. By virtue of an October, 2003, settlement agreement, $500,000 will be directed to fund indigent care programs, and the remainder will be paid to the government over two years. BNA Highlights, Oct. 8, 2003; Oct. 8, 2003, telephone conversation with United States Attorney’s Office (W.D. Mich).
\item \textsuperscript{18} United States v. United Memorial Hospital, No. 1:01-CR-238 (W.D. Mich., Jan. 8, 2003).
\end{itemize}
In July of 2003, the for-profit Alvarado Hospital Medical Center, Inc., along with Alvarado’s parent system and its CEO, were indicted on federal criminal charges concerning alleged violations of the Medicare Anti-Kickback Act in connection with alleged physician recruitment policies. Issues of the transparency of the hospital’s recruitment practices and the board’s role, if any, in approval of such practices no doubt will surface as this case progresses through the criminal justice system. While the merits of the case are as yet unresolved, and the defendants must be presumed innocent, this prosecution reaffirms that the Department of Justice (DOJ) has no timidity about prosecuting entities and their officers and directors in what it deems to be appropriate cases.

Finally, and directly related to the SOA, is the ongoing federal criminal investigation of HealthSouth, one of the nation’s largest healthcare services providers, with approximately 1,700 hospital, outpatient surgery, diagnostic imaging, and rehabilitative facilities nationwide. The investigation is focused on allegations that, in an effort to “manage earnings” to meet the earnings-per-share expectations of Wall Street analysts, HealthSouth management conspired to inflate assets and overstate earnings by between $1.4 and $2.7 billion through false and delayed accounting entries and bogus transactions.

To date, federal criminal charges have been filed against sixteen former HealthSouth executives, including HealthSouth’s former CEO and chairman of its board. The charges all revolve around fraud in financial reporting. Fifteen executives charged to date have pleaded guilty, including all five of the CFOs in the history of HealthSouth. As this paper went to press, sentences have been imposed on some relatively lower level executives ranging from probation with fines and restitution to five months in jail. The government has implied that it is working its way up the ladder of HealthSouth’s organizational chart; whether this criminal probe will stop in the higher reaches of HealthSouth’s former management or extend further into the board room is unknown.

For purposes of this white paper, it is important to note that in the HealthSouth investigation, for the very first time, the government has brought criminal charges based on

---

22 United States v. Scrushy, Crim. No. CR-03-BE-0530-S (N.D. Ala., Oct. 29, 2003). In addition to other penalties, the government is seeking $278 million in forfeiture from the defendant. Trial likely will occur sometime in 2004. The SEC also has filed a civil suit against HealthSouth’s former CEO and board chairman alleging a scheme to inflate profits. SEC v. HealthSouth and Scrushy, CA No. CV-03-J-0615-S (N.D. Ala. 2003).
23 Note that to the extent any alleged fraudulent activity affected the books and records of individual HealthSouth facilities, the veracity of the Medicare and Medicaid cost reports submitted by these facilities may also be implicated. To date, however, no criminal Medicare or Medicaid fraud-related charges have been filed.
on the SOA financial statement certification provision. HealthSouth’s former CEO and three former CFOs have been charged with, among other things, certifying to materially inaccurate reports of financial conditions and results of operations contained in HealthSouth quarterly reports (Form 10-Q) to the SEC.

As discussed below, the government has long been able to prosecute financial fraud under the criminal false statements statute, and under the mail, wire, bank, healthcare, and securities fraud statutes. Pinpointing individual liability within a corporation, however, is no easy task. Good faith reliance on others—subordinates, peers, accountants, and lawyers—can negate the knowledge, intent to defraud, willfulness, or scienter necessary to prove most of these crimes.

For at least two reasons, then, the SOA certification provisions discussed in this paper are important. First, they act to raise the consciousness of CEOs and CFOs to the importance of working hard to assure the integrity of the entity’s financial reporting mechanisms. CEOs and CFOs are now on notice. Second, as a result, the certification provisions can give regulators, agents, and prosecutors a “quick and dirty” way of reaching to the top of an organization, including its CEO and CFO who might otherwise be insulated from prosecution.

Little wonder then that in April of 2003, the Department of Health and Human Services (HHS) Office of Inspector General (OIG) partnered with the American Health Lawyers Association to produce the monograph, “Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors.”

26 Available at: http://oig.hhs.gov/fraud/complianceguidance.html.
II. PRE-SOA DISCLOSURE LAW AND RELATED CRIMINAL STATUTES

The requirement that a corporation honestly disclose its financial condition and honestly maintain its books, records, and internal accounting controls pre-dates the SOA. The government has long had an arsenal of weapons with which to sanction material misrepresentations or omissions regarding financial condition.

These older statutory weapons supplement those of the SOA. Of course, some pre-SOA statutes specifically target fraud in connection with publicly traded securities. The important point for healthcare counsel to note is that other predecessor federal fraud and false statement statutes, discussed below, are all-purpose statutes. They apply to fraud in all commercial spheres, including non-publicly traded for-profit and not-for-profit healthcare organizations.

A. SEC Filing-Related Statutes and Regulations

Among other required reports, publicly traded corporations must file annual (Form 10-K) and quarterly (Form 10-Q) reports with the SEC. These reports must contain financial statements, an analysis of financial condition, and results of operations in conformity with the SEC’s rules and regulations.

Under § 13 of the 1934 Securities Exchange Act, corporate books and records must be kept so that they “accurately and fairly” reflect, in “reasonable detail,” the company’s transactions and disposition of assets. The Act further provides that no person shall knowingly circumvent or knowingly fail to implement a system of internal accounting controls or knowingly falsify any book, record, or account.

A related SEC rule provides that annual and quarterly reports must contain, in addition to those disclosures expressly required by statute and rules, such other information as is necessary to ensure that the statements made in those reports are not, under the circumstances, materially misleading. These pre-SOA SEC rules also provide that no director or officer shall make or cause to be made a “materially false or misleading” statement to an accountant in connection with an audit or the preparation of any report to be filed with the SEC.

The Form 10-K must be signed by the registrant’s principal executive officer, principal financial officer, principal accounting officer, and by at least a majority of the board of directors; the Form 10-Q must be signed by an authorized officer and the principal financial officer.

---

28 15 U.S.C. § 78m(a); 17 C.F.R. §§ 240.13a-1, 240.13a-13 (Rules 13a-1 and 13a-13).
29 Id. at § 78m(b)(2)(a).
30 Id. at § 78m(b)(5); 17 C.F.R. § 240.13b2-1 (Rule 13b2-1).
31 17 C.R.F. § 240.12-20 (Rule 12b-20).
32 17 C.R.F. § 240.13b2-2(a) (Rule 13b2-2); see B. Carroll, Statements to Auditors, NATIONAL LAW JOURNAL, July 22, 2002, at B10.
financial or chief accounting officer.\textsuperscript{33} These signatures come under a certification that the report has been signed “pursuant to the requirements” of the Securities Exchange Act of 1934,\textsuperscript{34} which of course include the various prohibitions cited above.

Pre-SOA penalties, for any person who “willfully and knowingly” made or caused to be made in any report false or misleading statements with respect to any material fact, included a fine of up to $1 million ($2.5 million for corporations) and imprisonment for up to ten years.\textsuperscript{35} The SOA maintains this general prohibition on false and misleading statements but increases the penalties for violations of this law to fines of up to $5 million and twenty years imprisonment for individuals and a $25 million fine for corporations.\textsuperscript{36} Of course, under the \textit{ex post facto} clause, these higher penalties apply only to crimes committed after July 30, 2002.\textsuperscript{37}

B. General Securities Fraud

1. The Pre-SOA Securities Fraud Statutes

Fraud in connection with the sale of securities also has long been the subject of specific securities fraud statutes embedded in the Securities Act of 1933 and the Securities Exchange Act of 1934. The 1933 Act criminalizes the use of the mails or interstate commerce to accomplish a scheme or artifice to defraud, or to obtain money or property by means of any untrue statement or omission of a material fact, in connection with the offer or sale of a security. The 1933 Act also proscribes participation in any transaction, practice, or course of business designed to operate as a fraud or to deceive the purchaser.\textsuperscript{38} The 1934 Act makes it unlawful for any person by use of the mails or some other means of interstate commerce to “employ, in connection with the purchase or sale of any security...any manipulative or deceptive device or contrivance” in contravention of SEC rules.\textsuperscript{39}

The SEC’s well-known “Rule 10b-5” amplifies the 1934 Act prohibition:

\begin{quote}
It shall be unlawful for any person . . . by use of any means or instrumentality of interstate commerce or of the mails . . . (a) To employ any device, scheme, or artifice to defraud, (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statement made . . . not misleading, or (c) To engage in any act, practice, or course of business which operates . . . as a fraud or
\end{quote}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{33} Securities Exchange Act of 1934 Rule 15d-14(a); General Instructions for Form 10K at § D(2)(a) and Form 10Q at § G, available at: http://www.sec.gov/about/forms/secforms.htm.
\item \textsuperscript{34} \textit{Id.}
\item \textsuperscript{35} 15 U.S.C. § 78ff(a) (§ 32(a) of the Securities Exchange Act of 1934).
\item \textsuperscript{36} \textit{Id.}; SOA § 1106.
\item \textsuperscript{38} 15 U.S.C. § 77q(a).
\item \textsuperscript{39} 15 U.S.C. § 78j(b).
\end{itemize}
\end{footnotesize}
deceit upon any person, in connection with the purchase or sale of any security.\textsuperscript{40}

In order to make out a Rule 10b-5(b) misrepresentation violation in the context of financial disclosures, the government must demonstrate that, in connection with the purchase or sale of a security, the defendant engaged in material misrepresentations or omissions in a report to the SEC or to stockholders and that the defendant acted with scienter.\textsuperscript{41} The term “scienter” refers to “a mental state embracing intent to deceive, manipulate, or defraud.”\textsuperscript{42} The test for materiality is whether there is a substantial likelihood that under all circumstances, a reasonable shareholder would consider the omitted or misstated information significant in deciding upon a course of action.\textsuperscript{43}

A corporate officer or director,\textsuperscript{44} acting with scienter, who signs a document that is filed with the SEC that contains material misrepresentations, such as a fraudulent Form 10-K, \textit{regardless of whether he participated in the drafting of the document}, “makes” a statement and may be liable for fraud or for making a false statement.\textsuperscript{45} Some courts have noted that:

by placing responsibility on corporate officers to ensure the validity of corporate filings, investors are further protected from misleading information . . . [k]ey corporate officers should not be allowed to make important false financial statements knowingly or recklessly, yet still shield themselves from liability to investors simply by failing to be involved in the preparation of those statements. Otherwise the securities laws would be significantly weakened.\textsuperscript{46}

Thus, even before the SOA, the dissemination of materially false or misleading financial statements in connection with the sale or offering of stock created criminal and civil exposure for high-ranking corporate officers and board members. Nonetheless, as discussed below, the SOA adds a new general securities fraud law and a false certification law to the federal criminal code.

\section*{2. The SOA Securities Fraud Statute}

Essentially tracking the wording of the mail, wire, bank, and healthcare fraud statutes, the SOA securities fraud statute makes it a crime for:

\begin{itemize}
\item \textsuperscript{40} 17 C.F.R. § 240.10b-5.
\item \textsuperscript{41} Aaron v. SEC, 446 U.S. 680 (1980); Ernst & Ernst v. Hochfelder, 425 U.S. 185 (1976).
\item \textsuperscript{42} Aaron, 446 U.S. at 686.
\item \textsuperscript{43} TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438 (1976).
\item \textsuperscript{44} Even before the SOA, the SEC explained that “by signing documents filed with the Commission, board members implicitly indicate that they believe that the filing is accurate and complete.” “Audit Committee Disclosure,” SEC Release No. 41987 (Oct. 7, 1999).
\item \textsuperscript{45} See, e.g., Howard v. Everex Systems, Inc., 228 F.3d 1057 (9th Cir. 2000) (citations omitted).
\item \textsuperscript{46} Id. at 1061-62.
\end{itemize}
Whoever knowingly executes, or attempts to execute, a scheme or artifice—

(1) to defraud any person in connection with any security [of an issuer registered under § 12 of the 1934 Act or required to file reports under § 15(d) of that Act]; or

(2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any money or property in connection with the purchase or sale of any security [as defined in subsection (1)].

The maximum penalty for an SOA securities fraud violation is twenty-five years imprisonment and a fine of up to $250,000 ($500,000 for corporations).

There are some semantic differences between the “old” securities fraud laws and this new SOA securities fraud statute, but query whether these really are substantive differences. For example, proving deceit in connection with the purchase or sale of securities (old law) versus proving intent to defraud in connection with any security (SOA) seems unlikely to create much practical difference in the scope of cases that may be prosecuted.

The real import of this SOA securities fraud law may be its cultural impact within the Department of Justice, a factor that should not be dismissed or discounted. Securities fraud prosecutions typically were the domain of a relatively few, big city United States Attorney’s Offices with specialized knowledge of the Securities Exchange Act of 1934, the Securities Act of 1933, and the correlative criminal provisions found in Title 15 of the United States Code. These provisions were separate and apart from the vast bulk of the criminal code located in Title 18 and seemingly required knowledge of arcane SEC rules.

Now federal prosecutors have at their disposal an expansively worded securities fraud statute codified in the familiar realm of Title 18. The statute tracks the broad language of the mail, wire, bank, and healthcare fraud statutes by employing the more general “scheme to defraud” language that prosecutors are far more accustomed to charging and proving. Securities fraud is now “on the radar screen,” and it is predictable that DOJ will train its prosecutors and agents to bring actions under the new SOA securities fraud law.

Note that under the ex post facto clause, this law will apply only to criminal conduct committed after July 30, 2002. However, the statute appears to create a continuing offense, for a “scheme or artifice” may extend over time. It is not yet clear how a securities fraud scheme that straddles the effective date of the SOA will be treated. In the context of the similarly worded HIPAA healthcare fraud and bank fraud statutes,

---

48 Id.; 18 U.S.C. § 3571(b)(3), (c)(3).
some courts have held that each execution of the scheme, and not each act in furtherance of the scheme, is the punishable “unit of prosecution.”\(^{50}\) Accordingly, defense counsel must be alert to how the government crafts the scheme language of the indictment and seek to bar any schemes executed prior to the SOA on \textit{ex post facto} grounds. Alert prosecutors no doubt may counter by charging “straddle” schemes under the old Title 15 securities fraud laws as well.

\textbf{C. False Statements, Mail, and Wire Fraud}

Wholly apart from these securities-centered criminal statutes are the more traditional false statements and fraud statutes, which can apply to all healthcare entities, whether or not they are publicly traded.

The federal false statements statute is very broadly written. It makes it a crime to knowingly and willfully: (a) falsify, conceal or cover up by any trick, scheme or device a material fact; (b) make any materially false, fictitious or fraudulent statement or representation; or (c) make or use a document knowing it to contain any materially false, fictitious, or fraudulent statement or entry, “in any matter within the jurisdiction of the executive, legislative or judicial branches” of the federal government.\(^{51}\) Maximum penalties include five years imprisonment and a $250,000 fine ($500,000 for corporations).\(^{52}\) Thus, submission of a materially false or misleading report to the SEC, or indeed, to a bank providing a government-backed loan,\(^{53}\) can expose a company and its officers to criminal liability.\(^{54}\)

The mail and wire fraud statutes are similarly broad, and criminalize the use of the U.S. mails, interstate carriers, or interstate wires (including facsimiles and e-mails) to execute any scheme or artifice to defraud or to obtain money or property by means of false or fraudulent pretenses, representations, or promises.\(^{55}\) These statutes apply to any fraud, whether or not it is directed to the government or to investors. Pre-SOA, the maximum penalties for a mail or wire fraud violation were five years imprisonment and a $250,000 fine ($500,000 for corporations).\(^{56}\) The SOA increases the maximum penalty for each violation to twenty years imprisonment.\(^{57}\) Note also that if the fraud “affects” a financial institution, the penalties further increase to thirty years imprisonment and a $1 million fine.\(^{58}\)

---


\(^{52}\) 18 U.S.C. §§ 1001, 3571(b)(3), (c)(3).

\(^{53}\) See 18 U.S.C. §1014 (false statement to FDIC-insured institution).

\(^{54}\) See, e.g., \textit{United States v. Blizerian}, 926 F.2d 1285 (2d Cir.), \textit{cert. denied}, 502 U.S. 813 (1991) (false statement on forms filed with the SEC may be prosecuted under § 1001 or under more specific securities law provisions).

\(^{55}\) 18 U.S.C. §§ 1341, 1343.

\(^{56}\) \textit{Id.}; 18 U.S.C. § 3571(b)(3), (c)(3).

\(^{57}\) SOA § 903.

In this regard, note also that most not-for-profit organizations are required under the Internal Revenue Code to file informational returns using Form 990, which discloses the organization’s financial condition. The IRS Exempt Organizations Office reportedly intends to increase its enforcement presence via a new compliance unit used to review Form 990 returns. Of course, making a false filing with the IRS is a criminal offense itself.

Moreover, under federal law, Form 990 filings and applications for tax exemption must be made available for public inspection, on the Internet or otherwise. In many states, the Form 990 filing is often a part of the annual report required to be filed by charitable organizations with the state. Thus, false representations of financial condition to payors (e.g., in cost reports), lenders, bondholders, or even contributors could and still may be prosecuted under traditional mail or wire fraud theories.

D. Healthcare Fraud

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) created a far-reaching healthcare fraud statute that tracks the wording of the mail and wire fraud statutes but eliminated the requirement that the government prove a mailing or wire in furtherance of the fraud. The HIPAA statute specifically criminalized schemes or artifices to defraud, or to obtain money by means of false or fraudulent pretenses or promises, from any public or private “health care benefit program.” “Health care benefit program” is defined to include “any public or private plan or contract, affecting commerce, under which any medical benefit, item, or service is provided to any individual, and includes any individual or entity who is providing a medical benefit, item, or service for which payment may be made under the plan or contract.”

Given this expansive definition, a scheme to defraud public or private payors by employing false cost reports or claims could easily fall with the reach of the HIPAA

63 The public is tutored to look to these filings for information about not-for-profit organizations. See, e.g., How to Read the IRS Form 990 & Find Out What It Means (Nonprofit Coordinating Committee of New York, 2003), available at: http://www.npccny.org/Form_990/990.htm.
64 Fraud on banks could also be prosecuted under a separate bank fraud statute that tracks the wording of the mail and wire fraud statutes but eliminates the requirement of a mailing or a wire. 18 U.S.C. § 1344. Bank fraud carries maximum penalties of thirty years imprisonment and a $1 million fine. Id.
66 18 U.S.C. § 24(b) (emphasis added).
healthcare fraud statute. The maximum penalties for a healthcare fraud violation not causing bodily injury are ten years imprisonment and a $250,000 fine ($500,000 for corporations).  

E. Tax Exempt Bond-Related Disclosure Fraud

To date, Congress has exempted offerings of municipal securities from the registration requirements of the Securities Act of 1933 and from the reporting requirements of the Securities Exchange Act of 1934. Thus it appears that the SOA certification provisions are not directly applicable to municipal bond issuers and obligated entities. However, municipal securities transactions are still subject to the prohibitions of general commercial anti-fraud statutes as well as to the anti-fraud provisions of the 1933 and the 1934 Securities Acts.

Of course, not-for-profit entities, and occasionally for-profit affiliates, in the healthcare sector become involved in tax-exempt financings as the users of bond proceeds and the source of repayment, e.g., AHERF. These are often referred to as “conduit bonds” or “conduit financings,” which are defined as “municipal securities [that] are issued by a state or local government for the benefit of a private corporation or other entity that is ultimately obligated to pay such bonds.” The obligation to provide full and honest financial disclosure by the third party healthcare entity to bond issuers and brokers can create fertile ground for allegations of fraud, both at the point of initial offering and in the secondary market.

In 1995, the SEC amended its municipal securities disclosure securities rule, Rule 15c2-12, to effectively require, with some exceptions, hospital systems and other organizations borrowing the proceeds of tax-exempt debt, and obligated on that debt, to make annual disclosures of financial statements and significant events available to bondholders and potential investors. Apparently, some bond insurers are requiring quarterly audited financial statements; some bond-rating agencies are also doing quarterly and monthly reviews for signals of financial problems.

---

72 Disclosures are made to four Nationally Recognized Municipal Securities Information Repositories (MSIRs). Three states, Texas, Michigan, and Ohio, have their own repositories. Lists and addresses are available at: www.sec.gov/info/municipal/nrmsir.htm.
73 17 C.F.R. § 240.15c2-12(b)(5); for background, see SEC Release No. 34-34961 (Nov. 10, 1994).
Materially false representations in these Rule 15c2-12 disclosures potentially expose the entity to a Rule 10b(5) prosecution for fraud and deceit in connection with the sale of securities or to prosecution under the more general fraud statutes discussed above.75

III. SARBANES-OXLEY DISCLOSURE: THE “CIVIL” § 302 CERTIFICATION REQUIREMENT

Consistent with Congress's intent to increase the transparency and reliability of reports filed with the SEC and made available to the investing public, § 302 of the SOA (15 U.S.C. § 7241) requires that the principal executive and financial officers (CEOs and CFOs) of publicly traded companies certify the contents of their companies' periodic reports to the SEC. (§ 906 of the SOA, discussed in the following chapter, imposes criminal penalties for false certifications as to those reports.)

Unlike many provisions of the SOA that handed discretion over the details to the SEC, the § 302 certification requirements were set forth with great particularity in the Act itself. Accordingly (and as specifically required by the statute), very shortly after the SOA was passed in July, 2002, the SEC issued a proposed rule on the certification requirements and promulgated its final rule effective August 29, 2002. As noted by the SEC in its August 2002 final rulemaking, the text of the SOA largely dictated precisely what certification is required, and left the Commission little discretion. The SEC has further stated that the required statement cannot be waived, modified, or qualified, but must be adhered to strictly.

In June of 2003, the SEC amended certain of the certification requirements to permit investors easier access to both the § 302 certification and the separate § 906 certification, and to allow the Department of Justice to search a periodic report more expeditiously to verify that all the required certifications have been included. The 2003 amendments also incorporated new language in the § 302 certification itself, tied to the directives of § 404 of the SOA regarding reporting on internal controls over financial management.

A. Statutory Overview of § 302

Section 302 of the SOA addresses "Corporate Responsibility for Financial Reports," and directs the SEC to promulgate rules to require the principal executive officer and the principal financial officer of companies subject to the reporting requirements of the Securities Exchange Act of 1934 to certify their annual and quarterly reports to the SEC. Under the express terms of the Act, this certification must include detailed statements regarding the signing officers' knowledge of the accuracy of the report, specifically:

---

76 Reports filed with the SEC are publicly available at: http://www.sec.gov/edgar.shtml.
78 See 67 Fed. Reg. at 57,277 (explaining that the rules implement the certification mandated by the Act).
80 See 68 Fed. Reg. 36,635 (June 18, 2003).
81 See 15 U.S.C. §§ 78m, 78o(d).
(1) the officer has reviewed the report;

(2) based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances in which such statements were made, not misleading; and

(3) based on the officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report.

Moreover, the signing officers must declare that they are responsible for, and have established, maintained, and reviewed their company's systems of internal controls so as to ensure the accuracy of the company's reports, as follows:

(4) the signing officers--

(A) are responsible for establishing and maintaining internal controls;

(B) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;

(C) have evaluated the effectiveness of the issuer’s internal controls as of a date within 90 days prior to the report; and

(D) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date.

Finally, under this provision, the signing officers must certify that they have made certain disclosures to their company’s auditors, audit committee of their board of directors, and investors. By statute, the officers are required to certify that:

(5) the signing officers have disclosed to the issuer’s auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)—

(A) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer’s ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and
any fraud, whether or not material, that involves
management or other employees who have a significant role
in the issuer's internal controls; and

the signing officers have indicated in the report whether or not there
were significant changes in internal controls or in other factors that
could significantly affect internal controls subsequent to the date of
their evaluation, including any corrective actions with regard to
significant deficiencies and material weaknesses.

The Act instructs that the SEC's rules regarding these certification requirements
become effective thirty days after the enactment of the SOA.\textsuperscript{83}

Note that subsection 5(B) of § 302 requires that the officers certify that “any fraud,
whether or not material,” involving either management or employees with a significant
role in internal controls, has been disclosed not only to the board audit committee but
also to the company's outside auditors. To the extent this conduct has been discovered
via an internal investigation run through counsel, this required § 302 disclosure to
outside auditors arguably could work a waiver of the attorney-client privilege as to
aspects of that investigation.\textsuperscript{84} How to conduct such investigations, and whether and
how to make such a disclosure, must be weighed carefully to minimize the risk of a
privilege waiver.

\textbf{B. Regulatory Overview of § 302}

Pursuant to the statutory mandate of § 302, the SEC announced its final rule regarding
"Certification of Disclosure in Companies' Quarterly and Annual Reports," in late
August, 2002.\textsuperscript{85} The commentary to this rulemaking noted that the SEC had proposed
rules in June of 2002 that would have required CEOs and CFOs to certify the contents
of their companies' periodic reports and also would have required companies to
maintain procedures for assuring the disclosure of information required by the reports.
Moreover, the SEC's June proposal would have required companies to undertake an
annual evaluation of their procedures under the supervision of company management.
However, these proposals, and the comments that they engendered, were superseded
by the Congressional mandate of the SOA. Accordingly, the final rule announced in
August implemented the certification required by the Act, instead of the proposals
previously offered by the Commission.\textsuperscript{86}

\textsuperscript{83} See 15 U.S.C. § 7241(c) (SOA § 302(c)). The Act also provides that the certification requirement
applies to CEOs and CFOs of banks and savings associations that file periodic reports with the SEC, as
well as to foreign issuers. 15 U.S.C. § 7241(b) (SOA § 302(b)).

\textsuperscript{84} Note that there is no federal accountant-client privilege. United States v. Arthur Young & Co., 465 U.S.

\textsuperscript{85} 67 Fed. Reg. 57,276 (Sept. 9, 2002).

\textsuperscript{86} \textit{Id.} In response to the June proposed rulemaking, the Commission received nearly 100 comment letters
from individuals, companies, associations, and members of the accounting and legal communities.
The August 2002 final rule amended Exchange Act Rules 13a and 15d to include the SOA certification requirements for reports filed pursuant to §§ 13(a) and 15(d) of the Securities Exchange Act of 1934. The requirement pertains to annual reports made on SEC Forms 10-K, 10-KSB, 20-F, and 40-F, and to quarterly reports on SEC Forms 10-Q and 10-QSB. It also applies to any amendments of those reports, and to any transition reports.

Initially, the content of the § 302 certification requirement largely tracked the statutory language. Acknowledging Congress's apparent intent to be sweeping in its SOA reforms, however, the Commission translated the Act's reference to "internal controls" expansively in its August 2002 rulemaking. There, the SEC created the category of disclosure internal controls and procedures, and defined that category to encompass both financial and non-financial information included in a company's periodic reports to the SEC. Subsequently, in June 2003, the SEC announced final rules, promulgated pursuant to § 404 of the SOA, regarding corporate management's obligation to report specifically on a company's financial reporting internal controls and procedures. In light of these rules, the Commission amended the § 302 certification requirements to specify that CEOs and CFOs must certify to both categories of internal controls and procedures. Per the June 2003 rulemaking, the certification language now includes a separate statement regarding the signing officers' knowledge of and responsibility for the company's internal controls and procedures for financial information. CEOs and CFOs must attest to this statement in addition to the broader certification regarding the company's disclosure controls and procedures.

The June 2003 final rule further included revisions to the form and location of the § 302 certification, which is now required to be filed as a separate exhibit to the relevant reports. As of this writing, the current certification regulations are summarized more fully as follows.

1. **Content of Certification**

The certification required by regulation incorporates the precise language of the statutory mandate of the SOA, with some exceptions consisting of additional language that is "consistent with Congressional intent." Per the regulations, CEOs and CFOs must certify first that the periodic reports themselves are materially accurate and

---

87 See 15 U.S.C. § 78m(a) (annual and quarterly reports required of registered issuers of security); 15 U.S.C. § 78o(d) (supplemental and periodic reports for issuers that have filed a registration statement).
89 See, e.g., 67 Fed. Reg. at 57,279 (noting adoption of statutory language with some exceptions to effectuate Congressional intent).
91 The June 2003 rulemaking also made minor modifications to the certification form, and those changes became effective as of August 14, 2003. However, as the additional language regarding financial controls and procedures was a substantive modification, the obligation to include this statement in the certification becomes effective at the time a company is required to comply with the requirement of a management report on financial controls, i.e., beginning in fiscal year 2004. See id.
92 Id.
complete. This certification is consistent with pre-existing statutory disclosure standards for "materiality" of disclosures.\textsuperscript{93} Second, the officers must certify that the financial information and data included in the report provide a "fair presentation" of the company's financial condition, results of operations and cash flows.\textsuperscript{94} This portion of the certification requirement is specifically not limited by reference to generally accepted accounting principles (GAAP): "We believe that Congress intended this statement to provide assurances that the financial information disclosed in a report, viewed in its entirety, meets a standard of overall material accuracy and completeness that is broader than financial reporting requirements under generally accepted accounting principles."\textsuperscript{95}

Following the June 2003 amendments, signing officers must also certify that they, in conjunction with the obligation of management to report on internal controls over financial reporting, are responsible for designing (or having designed) the company's financial reporting controls and procedures.\textsuperscript{96} The term "internal control over financial reporting," incorporated into the § 302 certification, is defined by the SEC in its § 404 management report regulations, and specifically relates to the preparation of financial statements for external purposes "in conformity with generally accepted accounting principles."\textsuperscript{97} Therefore, with respect to financial reporting, GAAP does apply; however, these standards do not necessarily address the "disclosure controls" that are also required and must be attested to per the certification.\textsuperscript{98}

Specifically, by both statute and regulation, the officers signing the § 302 certification must aver their ongoing oversight of these "disclosure controls." The regulations define the term "disclosure controls and procedures" to encompass broadly a set of controls and procedures that are designed to ensure the quality and timeliness of the disclosure requirements, including both financial and non-financial information.\textsuperscript{99} Otherwise, the §


\textsuperscript{94} \textit{Id.} The Commission added the specific reference to cash flows, even though not set forth in § 302 of Sarbanes-Oxley, believing that inclusion of this factor is consistent with Congressional intent.

\textsuperscript{95} \textit{Id.} The Commission further commented that, in its view, a "fair presentation" of a company's financial condition and results of operations and cash flows includes the selection and application of appropriate accounting policies in each company's particular circumstances. The stated goal is to have companies disclose information that reasonably reflects the true nature of underlying transactions and events that are reflected in the financial data, thus providing investors with a "materially accurate and complete picture" of the company's finances.

\textsuperscript{96} See 68 Fed. Reg. 36,635 (Jun. 18, 2003).

\textsuperscript{97} \textit{Id.}

\textsuperscript{98} The Commission's commentary provides little guidance on when and how to report information that is not addressed by GAAP. If faced with a close call on non-GAAP disclosures, a company may wish to seek further guidance from the SEC's accounting staff.

302 regulations do not prescribe any particular kind or form of disclosure controls and procedures that are required.100

2. Form and Location of Certification

In its August 2002 rulemaking releases, the SEC made clear that the certification required under the amended Exchange Act Rules must be in the exact form prescribed: "The wording of the required certification may not be changed in any respect (even if the change would appear to be inconsequential in nature)."101 Moreover, the officers charged with making the certification may not delegate that responsibility and are not permitted to have the certification signed on their behalf, under power of attorney or otherwise.102 It is apparent that the certification requirement is an attempt to hold individual corporate officers personally accountable, and potentially liable, for statements, misstatements, and omissions in their companies' reports.

Following its August 2002 final rulemaking, the SEC amended its annual and quarterly reporting forms to conform to the SOA directive that the certification be included "in" each report. Initially, the certification was to follow immediately after the signature sections of the reports. In June of 2003, the SEC revisited this format, and concluded that the § 302 certification should appear and be included as a separate exhibit to a company's periodic reports.103

The primary purpose of the 2003 amendments to the form and location of the requisite certifications is to "enhance the ability of investors, the Commission staff, the Department of Justice and other interested parties to easily and efficiently access the certifications" through the SEC's on-line database system,104 and "facilitate better monitoring of a company's compliance with the certification requirements."105

C. Comparing the § 302 Certification to Other Routine Certifications in the Healthcare Industry

Although many healthcare providers are accustomed to providing certifications on their reports, claims, and submissions to the government, the Sarbanes-Oxley certifications are different in complexity, rigidity, and tone.

---

100 However, in the June 2003 amendments to the certification, the SEC specified that the signing officers must evaluate their company's disclosure controls "as of the end of the period" covered by the report. See id.
102 Id. at 57,280, n. 63.
103 68 Fed. Reg. 36,635 (Jun. 18, 2003). The amendments also added a statement that the principal executive and financial officers are responsible for designing internal controls and procedures for financial reporting, clarifying that those internal controls, as well as disclosure controls and procedures, may be designed under the supervision of the signing officers, and revising the certification accordingly.
For example, a typical certification on a Certificate of Medical Necessity contains a brief statement that requires a certifying physician to aver that: "the medical necessity information in [the form] is true, accurate, and complete, to the best of my knowledge, and I understand that any falsification, omission, or concealment of material fact in [the form] may subject me to civil or criminal liability." Similarly, a nursing home cost report form requires an officer or administrator to review the report and certify that "[t]o the best of my knowledge and belief, they are true and correct statements from the books and records of the [facility] in accordance with applicable instructions, except as noted (attach a statement with exception if necessary)."

Similarly, a nursing home cost report form requires an officer or administrator to review the report and certify that "[t]o the best of my knowledge and belief, they are true and correct statements from the books and records of the [facility] in accordance with applicable instructions, except as noted (attach a statement with exception if necessary)."

In part because of this "knowledge and belief" language, in traditional false certification prosecutions, the government's most difficult burden is proving the intent of the individual who has signed the certification. A signing officer's good faith reliance on subordinates, particularly on those who actually gather the data and prepare the claims or reports, typically suffices to negate the intent requirements for civil or criminal prosecution.

The SOA § 302 certification language, however, is substantially more detailed and specific than other kinds of certifications seen within the healthcare industry. The SOA certification provides little leeway in terms of reasonable knowledge and belief. Although the § 302 certification requires the signer to aver "[b]ased on my knowledge," it further requires the signer to attest that he or she is responsible for establishing and maintaining disclosure controls and internal controls over financial reporting so as to ensure that "material information relating to the company . . . is made known to us," and to provide "reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements." The signer must represent, without caveat, that he or she has put procedures and controls in place to assure that information that is or should be contained in the company's reports is brought to light. It is based on this level of disclosure and reporting that the signer is then to attest to the accuracy and completeness of the reports "based on my knowledge." Functionally, despite initial appearances, this meager caveat provides much less protection for the individual CEOs and CFOs who must sign the certifications.

Also, in the context of routine Medicare and Medicaid certifications, healthcare providers typically have been able to alter or caveat the language of their certifications to provide at least some level of protection to the person signing. For example, a healthcare provider who is being questioned about certain costs, expenses, or practices can still meet the technical requirement of certifying statements or reports to the government,

---

106 See Form HCFA 484 (11/99) (Certificate of Medical Necessity – oxygen DMERC).
108 See, e.g., 17 C.F.R. § 220.601(b)(31) (description of Rule 13a-14(a) and Rule 15d-14(a) certifications).
109 See id.
while admitting that the signer’s knowledge may not be as broad, deep, or direct as the standard certification language suggests.  

With the SOA § 302 certification, however, the SEC has explicitly noted that the signing officers must use the precise language required by the reports. No modifications or changes will be accepted, regardless of how seemingly trivial. Moreover, whereas many reporting forms allow the certification to be signed by an appropriate corporate officer or proxy, the Sarbanes-Oxley certifications must be made by the principal executive officer and by the principal financial officer for the company. These individuals cannot avoid this obligation by appointing another officer or company representative to sign the certification exhibit.

In essence, the certification requirement is strictly enforced and must be adhered to precisely. This reflects the SEC’s view that Congress intended to assign responsibility for the company’s reporting compliance to the highest levels of corporate management, and did not wish to consider or permit loopholes that might provide individual CEOs or CFOs with a sustainable defense to allegations of wrongdoing or misstatement.

---

110 For instance, companies under investigation have been able to amend certification language to specify that the certification was believed to be accurate as of a particular date, not the date of signature, or to specify that the certification is made in reliance upon the representations of others within the company.  

IV. SARBANES-OXLEY DISCLOSURE: THE “CRIMINAL” § 906 CERTIFICATION REQUIREMENT

A. Statutory Overview of § 906

Prior to the SOA, no federal criminal statute was specifically directed to false certifications by a CEO or CFO. There was and is a general criminal false statements statute,\(^\text{112}\) and there also existed a general requirement that SEC filings be signed by officers, but those “signing requirements did not include any type of certification or other attestation regarding the accuracy or completeness of the report.”\(^\text{113}\) § 906 of the SOA (18 U.S.C. § 1350) fills that gap. It creates a criminal statute requiring CEOs and CFOs to certify to the material accuracy of any periodic reports to the SEC containing financial statements. This new criminal statute provides:

§ 1350. Failure of corporate officers to certify financial reports

(a) Certification of periodic financial reports. Each periodic report containing financial statements filed by an issuer with the Securities Exchange Commission pursuant to § 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a) or 78o(d)) shall be accompanied by a written statement by the chief executive officer and chief financial officer (or equivalent thereof) of the issuer.

(b) Content. The statement required under subsection (a) shall certify that the periodic report containing the financial statements fully complies with the requirements of § 13(a) or 15(d) of the Securities Exchange Act [of] 1934 (15 U.S.C. 78m or 78o(d)) and that information contained in the periodic report fairly presents, in all material respects, the financial condition and results of operations of the issuer.

(c) Criminal penalties. Whoever—

(1) certifies any statement as set forth in subsections (a) and (b) of this section knowing that the periodic report accompanying the statement does not comport with all the requirements set forth in this section shall be fined not more than $1,000,000 or imprisoned not more than 10 years, or both; or

(2) willfully certifies any statement as set forth in subsections (a) and (b) of this section knowing that the periodic report accompanying the statement does not comport with all the requirements set forth in this section shall be fined not more


than $5,000,000, or imprisoned not more than 20 years, or both.\textsuperscript{114}

This statute actually creates two separate crimes: one for knowingly and one for willfully non-compliant certifications. These SOA certification crimes can be made out without regard to any intended or actual gain to the CEO or CFO, or impact on stock prices. As § 1350 is a criminal statute, the DOJ, not the SEC, has enforcement authority.

It should be pointed out that this criminal provision imposes certification obligations separate and independent than those imposed by the civil § 302 certification, discussed above. Thus § 906 of the SOA creates a self-operative certification requirement subject to criminal penalties, effective immediately and applicable to offenses committed on or after the Act's passage on July 30, 2002.

Unlike the SOA § 302 certification requirement, § 906 does not specify particular wording for this certification. However, the regulations now direct that a company's § 906 certification should be “furnished” as exhibits and made publicly available in connection with periodic reports that contain financial statements.\textsuperscript{115}

Commentators have noted that SOA § 302 imposes broader certification requirements than does SOA § 906 (18 U.S.C. § 1350), as § 302 imposes certification requirements as to the design, effectiveness and deficiencies of a corporation's financial and disclosure controls. It is worth noting, however, that SOA § 906 actually contains a very inclusive, two-part certification. The CEO and CFO together must certify that: (1) the report including the financial statements “fully complies” with the requirements of §§ 13a and 15d of the 1934 Securities Exchange Act, and (2) the report fairly presents, in all material respects, the financial condition and results of operation of the corporation.

The requirements of § 13a and 15d of the 1934 Act, incorporated by reference in § 1350, include filing reports in accordance with the SEC’s rules and regulations. Those rules and regulations, including SEC Rules 13a-14(a) and 15d-14(a), require the filing of SOA § 302 certifications. Thus an SOA § 906 certification of “full compliance” with §§ 13a and 15d of the 1934 Act might be read to certify the filing of a report containing an accurate SOA § 302 certification as well. It is by no means clear that Congress intended this result by creating two different certification requirements. However, it is at least arguable that a false SOA § 302 certification regarding matters other than the corporation’s financial condition or the results of operations could be viewed by an aggressive prosecutor as a ground for a § 1350 prosecution. Of course, a knowingly

\textsuperscript{114} 18 U.S.C. § 1350 (SOA § 906) (emphasis added).

\textsuperscript{115} See 68 Fed. Reg. 36,635 (June 18, 2003). The terms of the SOA require only that the § 906 certification “accompany” periodic reports to the SEC that contain financial statements. By way of comparison, the § 302 certification must be included "in" the filed periodic report itself. As the § 906 certification need not be "filed" with the SEC, § 906 certifications are not subject to liability under § 11 of the 1933 Securities Act, 15 U.S.C. § 77k, or § 18 of the 1934 Securities Exchange Act, 15 U.S.C. §78r. However, the SEC made clear in its discussion that it expects § 906 certifications to be made available to the public.
false § 302 certification also could be prosecuted under the more traditional false statements or fraud statutes discussed above.

Finally, note that while the codified SOA § 906 (18 U.S.C. § 1350) is captioned “Failure of corporate officers to certify financial reports,” the statute does not on its face criminalize the failure to furnish a § 906 certification. However, the SEC staff has stated the position that “[a]n individual who [files a report but who] willfully fails to submit a certification required by § 1350 may be subject to criminal prosecution under § 32116 of the Securities Exchange Act” for filing a materially false report.117 In addition, the failure to furnish a § 906 certification could be construed as causing the periodic report to which it relates to be incomplete, thus arguably violating § 13(a) of the 1934 Securities Exchange Act.118

B. Analysis of Criminal Liability Under SOA § 906

1. State of Mind

A chief ambiguity in the statute is its distinction between submitting a certification “knowing” that it does not meet the requirements set out in § 1350 and “willfully” submitting a certification “knowing” that it does not meet the requirements set out in § 1350.119 As we have seen, a large swing in the maximum penalties appears to hinge on this distinction.

A seminal discussion about state of mind in criminal prosecutions is found in the Supreme Court’s opinion in Bryan v. United States.120 The Bryan court noted that “knowing” does not refer to a culpable state of mind or to knowledge of the law but to factual knowledge.121 The term “knowingly” merely requires proof of the defendant’s knowledge of the facts that constitute the offense.122 Thus, in the criminal law context, the word “knowing” is commonly used to distinguish volitional conduct from conduct that is unwitting or accidental.

By contrast, the word “willful” is meant to describe a culpable state of mind with regards to the law. The Supreme Court defined “willful” as an act undertaken with a bad purpose, i.e., with knowledge that the conduct was unlawful.123 The Court went on to recognize that in rare cases involving highly technical, usually regulatory, statutes that

118 Id. at § II(B), 4.
119 One commentator suggests that this ambiguity may rise to the level of a Due Process “notice” deficiency. Terwilliger, G., Business Regulation: Commerce and Crime, NATIONAL LAW JOURNAL Jan. 27, 2003. The matter has yet to be litigated.
121 Id. at 192-93.
122 Id. at 193.
123 Id. at 191.
present the danger of “ensnaring” individuals engaged in apparently innocent conduct, it had defined “willfully” to further require that the defendant have knowledge of the actual law forbidding that conduct.124

Using the Bryan template, a “knowing” SOA § 906 violation would mean a certification submitted knowing the facts that constitute the offense. For this offense, that would mean a certification submitted while knowing that it either did not fully comply with the particular requirements of §§ 13a and 15d of the 1934 Act or did not otherwise fairly present in all material respects the corporation’s financial condition and operational results. A “willful” SOA § 906 violation would mean both (1) submitting a certification knowing that it did not fully comply with the requirements of §§ 13a and 15d of the 1934 Act or otherwise fairly present in all material respects the corporation’s financial condition and operational results and (2) making that submission with bad purpose or knowing that it was unlawful.

Yet in this context, this seems to be a distinction without a difference. How could a CEO or CFO in the year 2004 knowingly submit a non-compliant SOA § 906 certification and not also know that such a submission was unlawful? Beyond the publicity given to this certification requirement in the general and legal media, the form of certification suggested by many law firms on their web sites declares the certification to be “pursuant to 18 U.S.C. § 1350, as adopted pursuant to § 906 of the Sarbanes-Oxley Act of 2002.” A knowing submission of a non-compliant certification “pursuant to § 1350” seemingly would indicate knowledge that the submission was unlawful almost by definition. Thus, should a prosecution under § 1350 proceed to indictment and trial, it is likely that the government would seek to charge the more serious “willful” offense.

The provision for a separate “knowing” crime in the statute may serve two practical purposes. First, in the case of guilty plea or cooperation agreements with the government, the government may allow the defendant to plead to a “knowing violation” and thus limit the defendant’s maximum prison exposure at ten years. This was done in the case of several former HealthSouth CFOs who pleaded guilty and are cooperating with the government.125 By contrast, the recently indicted former HealthSouth CEO is charged with a “willful” violation of § 1350.126 Second, in the case of a trial, it may allow counsel to seek a lesser-included offense instruction and so permit a jury compromise.

2. Defenses

By requiring CEOs and CFOs to certify to the adequacy of financial and disclosure controls under SOA § 302, as well as to certify to filings in compliance with securities laws and to the material fairness and accuracy of financial statements and reports of

124 Id. at 194-95 (e.g., statutes criminalizing structuring money laundering transactions and certain tax violations).
operations, Congress appears to be seeking to undercut traditional white collar defenses centering on an executive’s mistake, insulation from the alleged bad acts of subordinates, or reliance on others, including experts.

Plainly, a true mistake would not rise to the level of a knowing certification, much less one submitted willfully. Similarly, if one truly is misled about material facts as to which a certification later is submitted, then he or she cannot have the requisite knowledge to sustain a conviction. Finally, good faith reliance on an expert, to whom all relevant facts have been disclosed, may still be a defense to a false certification charge.127

Yet, the conjunction of the SOA’s implicit due diligence requirements and the criminal law doctrine of reckless disregard makes all of these defenses that much harder to sustain. It has long been the law in securities fraud cases and elsewhere that reckless disregard of the truth or conscious avoidance of the truth can make out the knowledge necessary to sustain a criminal conviction.128 Sciento for a securities fraud violation may be established by a showing of either knowing misconduct or severe recklessness.129 Proof of recklessness ordinarily requires a showing that the defendant’s conduct exhibited an extreme departure from the standards of ordinary care, creating a danger of misleading buyers or sellers, that is either known to the actor or is so obvious that the actor must have been aware of it.130 This could include deliberately seeking to shield oneself from liability by failing to get involved in the preparation of a financial report.131

The SOA now places the CEO and CFO ever more squarely on the front lines not only of accurately reporting operating results but of ensuring the integrity of the information systems and internal controls that generate the data used to report those results. To the extent these officers do not make a concerted effort both to ask the right questions and to document that those questions were asked and how they were answered, they place themselves in jeopardy of a reckless disregard allegation.

This resulting drive to document the process by which the certified information is generated apparently has led CEOs and CFOs to require “sub-certifications” by financial and other professionals within the corporation who contribute to the information that appears in SEC reports. This has caused some consternation among such subordinates.132 It also creates potential criminal exposure for those subordinates.


129 See, e.g., SEC v. Carriba Air, Inc., 681 F.2d 1318 (11th Cir. 1982).

130 See, e.g., SEC v. Southwest Coal and Energy Co., 624 F.2d 1312 (5th Cir. 1980).


The federal criminal code contains the crimes of conspiracy and aiding and abetting. Arguably, a subordinate who falsely sub-certifies in concert with others may be exposed to a charge of conspiring to submit, or aiding and abetting the submission of, a false SOA § 906 certification. Moreover, while the maximum prison term for criminal conspiracy formerly was capped at five years, the SOA pegs the maximum sentences for conspiracy to violate the mail, wire, bank, healthcare, and securities fraud statutes, and for conspiracy to file non-compliant SOA § 906 certifications, to the much higher maximum sentences of those substantive offenses.

Apart from these mistake and reliance defenses, made more difficult by the SOA’s implicit imposition on CEOs and CFOs of heightened due diligence obligations, there also exists some room to defend based on statutory or regulatory ambiguity. An SOA § 906 certification requires certification that the report “fully complies” with cited sections of the 1934 Act. It also requires certification that the report “fairly presents,” in all material respects, financial condition and operational results. But what does “full compliance” or “fair presentation” mean in this context? If one has to “know” that a report does not “fully comply” with all of the requirements of the cited sections of the Act in order to be criminally liable, then a good faith belief that the report does comply, at least materially or substantively, may well furnish a defense.

With reference to “fair presentation” of financial condition and operational results, the SEC staff takes the position for purposes of an SOA § 302 certification that “Congress intended the [certification] statement to provide assurances that the financial information disclosed in a report, viewed in its entirety, meets a standard of overall material accuracy and completeness that is broader than financial reporting requirements under generally accepted accounting principles [GAAP].” Presumably, DOJ would make the same argument regarding SOA § 906. In short, the determination of knowing compliance with the fair presentation standard will be fact driven, which could be vulnerable to a good faith reliance defense.

Finally, if “full compliance” with a regulation or rule is contested but the regulation is itself susceptible to more than one reasonable interpretation, this too may constitute a defense to an SOA certification crime. Several cases set in the context of the False Claims Act (FCA) have made a similar point. So long as one acts on a reasonable interpretation of a regulation, taking advantage of a disputed legal issue in submitting a claim does not constitute the knowledge or reckless disregard required under the FCA. Similarly, even if one is on notice that the government (or even one’s own consultants) think that a particular regulatory requirement exists regarding cost reports, taking action contrary to that view does not necessarily establish FCA knowledge and.

---

willfulness, unless the government can prove that one acted under an unreasonable interpretation of the law.\(^{138}\)

It seems fair to say that despite its ambiguities and notwithstanding potential defenses, the SOA § 906 criminal certification requirement does and will exert an unprecedented \textit{in terrorem} effect on CEOs and CFOs of publicly traded companies. In combination with other compliance signals—DHHS OIG compliance guidance, the federal sentencing guidelines for organizations, the actions of state attorneys general, and pressures from gatekeepers and other involved players like auditors, lenders, D & O insurers, bond rating agencies, investors, and donors—SOA certification likely heralds a new era in corporate governance for non-publicly traded organizations as well.

\section{Criminal Penalties}

As noted above, the maximum penalties for violating the SOA § 906 certification provision are ten years in prison and a $1 million fine or twenty years in prison and a $5 million fine depending on whether the violation is knowing or willful.\(^{139}\) These are statutory maximums. The actual prison term and fine that a defendant receives for a fraud offense or false certification offense is determined by the sentencing judge with reference to the United States Sentencing Guideline for “Offenses Involving Fraud or Deceit.”\(^{140}\)

The federal sentencing guidelines essentially create a matrix of imprisonment ranges using an “offense level” (based on specified offense characteristics) on one axis and offender criminal history score on the other. The judge must sentence within the specified guideline range absent unusual factors, which justify upward or downward departures from that range. For the fraud guideline, the driving offense factor is actual or intended loss caused by the crime. Enhancements to the offense level ratchet up according to the dollar amount of such loss and the presence of other specified offense characteristics.\(^{141}\)

At the time SOA was enacted, the fraud sentencing guidelines were not exactly lenient. Fraud and other white collar offenders constituted about 17.5% (10,471 individuals) of all the federal offenders sentenced in 2001.\(^{142}\) In that year, the average length of imprisonment for federal fraud offenses was 18.7 months.\(^{143}\) Nonetheless, the SOA mandated that the United States Sentencing Commission “review and amend, as appropriate,” the guidelines for obstruction of justice, accounting and financial fraud, and penalties for organizations.\(^{144}\)

\(^{138}\) \textit{See United States v. Whiteside}, 285 F.3d 1345 (11th Cir. 2002).
\(^{139}\) 18 U.S.C. § 1350.
\(^{140}\) U.S.S.G. § 2B1.1.
\(^{141}\) \textit{Id.} at § 2B1.1(b).
\(^{142}\) United States Sentencing Commission, Office of Policy Analysis, 2001 Datafile, OPAFY01.
\(^{143}\) \textit{Id.}
The Commission responded with a report,\textsuperscript{145} “emergency” Guideline amendments effective January 25, 2003, and additional amendments that became effective on November 1, 2003. The upshot of this activity is that the fraud guidelines for an offender have been boosted in dramatic ways for offenses occurring after the effective date of the particular guideline amendment. For example, the base offense level for fraud and false certifications has been raised one level to an offense level seven, if the underlying crime has a maximum prison penalty of twenty years or more.\textsuperscript{146} This will reach the new SOA crimes of securities fraud, 18 U.S.C. §§ 1348, and willful false SOA § 906 certifications, 18 U.S.C. § 1350. The effect of this seemingly small amendment is to narrow the availability of a pure “Zone A” probation sentence, assuming a two-level credit for acceptance of responsibility, to frauds causing losses of $10,000 or less rather than $30,000 or less as was previously the case.\textsuperscript{147} Similarly, a “Zone D” sentence of incarceration now is mandated if the fraud loss is more than $70,000, whereas previously the fraud loss had to exceed $120,000 for a similar result.\textsuperscript{148}

In addition, the guideline provides for a four-level enhancement if the offense violates securities laws and was committed by an officer or director of a publicly traded company.\textsuperscript{149} The Application Notes to this guideline explicitly provide that “securities laws” in the context of this enhancement includes violations of §§ 1348 and 1350 as well violations of more general fraud laws involving securities.\textsuperscript{150} Thus, the sentencing guideline calculation for an SOA § 906 false certification conviction starts at an offense level of eleven. Assuming no prior convictions, a level eleven corresponds to an imprisonment range of 8-14 months without factoring in any monetary loss.

Yet in securities fraud cases, the fraud loss calculated by the government is almost always substantial. Depending on the amount of that loss, and on other offense characteristics such as the number of victims and the like, the offense level and sentencing range can skyrocket. For example, a fraud loss of $201,000 adds twelve levels (a 46-57 month prison range), a loss of $1,000,001 adds sixteen levels (a 70-87 month prison range), and so forth.

This revised fraud guideline also makes clear that the calculation of loss includes any reduction in the value of equity securities or other corporate assets.\textsuperscript{151} In addition, the guideline contains new offense level enhancements pegged to the number of victims.

\textsuperscript{146} U.S.S.G. § 2B1.1(a) (eff. Nov. 1, 2003).
\textsuperscript{147} U.S.S.G. § 5B1.1(a).
\textsuperscript{148} U.S.S.G. § 5C1.1.
\textsuperscript{150} Id. at § 2B1.1, App. Note 11 (eff. Jan. 25, 2003).
\textsuperscript{151} Id. at § 2B1.1, App. Note 2(C)(iv) (eff. Jan. 25, 2003).
(over 10, 50, or 250)\textsuperscript{152} and to whether the solvency or financial security of a publicly traded organization, or of one hundred or more victims, is substantially endangered.\textsuperscript{153}

Thus, the sentencing guideline range for any particular violation of the SOA § 906 certification law will depend largely on the extent to which the government can link that false certification to a larger pattern of relevant conduct by the offender or co-conspirators that causes losses and creates victims. However, note that even in a “no loss” case, the Application Note to the fraud guideline encourages judicial and prosecutorial consideration of “upward departures” from the offense level determined under that guideline, where the level “substantially understates the seriousness of the offense.”\textsuperscript{154}

Moreover, at the same time that fraud guidelines are being boosted, guideline downward adjustments and downward departures that once were available to white collar defendants are being cut back, more stringent appellate review of such departures has been mandated, and the government’s charging and plea bargaining policies have been made more restrictive.

- First, by direct Congressional amendment of the guidelines via the PROTECT Act,\textsuperscript{155} effective April 30, 2003, and by Commission guideline amendments effective October 27, 2003, made in response to the directives of that Act, a number of grounds for sentencing guideline downward departures now are prohibited: “super-acceptance” of responsibility, minor role in offense, gambling addiction, and repayment of legally required restitution. In addition, the availability of departures based on family ties and responsibilities and on aberrant behavior are limited.\textsuperscript{156} In light of these changes, defense counsel must be alert to \textit{ex post facto} arguments based on the effective date of the particular amendment at issue.

- Second, on April 30, 2003, provisions of the PROTECT Act\textsuperscript{157} changed the applicable standard of review on aspects of appeals from departures from the sentencing guidelines, including, of course, government appeals from downward departures granted to white collar defendants. The courts of appeals now are to review \textit{de novo} a sentencing court’s application of the guidelines to the facts to ensure that a downward departure is authorized under the law and justified by the facts of the case.\textsuperscript{158} This is a sea change from the prior “abuse of discretion”

\textsuperscript{152} \textit{Id.} at § 2B1.1(b)(2) (eff. Jan. 25, 2003).

\textsuperscript{153} \textit{Id.} at § 2B1.1(b)(12) (eff. Nov. 1, 2003).

\textsuperscript{154} \textit{Id.} at § 2B1.1, App. Note 16 (eff. Jan. 25, 2003).


\textsuperscript{158} 18 U.S.C. § 3742(e) (amended eff. April 30, 2003).
standard,\textsuperscript{159} and can be bad news for white collar defendants. Courts have already begun to reverse downward departures in healthcare fraud prosecutions that previously might have been upheld.\textsuperscript{160} Defense counsel no doubt should seek to pose the issue on appeal as a finding of fact still subject to a clearly erroneous standard.\textsuperscript{161}

- Third, the Attorney General recently has directed federal prosecutors, with limited exceptions, to charge, and accept guilty plea agreements to, only the most serious and readily provable offense. In other words, there can be no charge bargaining.\textsuperscript{162} Moreover, prosecutors may not fact bargain with defendants about issues affecting guideline offense level enhancements, e.g., amount of loss, and they should rarely acquiesce in downward departures from the guideline range other than for substantial assistance in the investigation and prosecution of another person.\textsuperscript{163} Therefore, if conviction seems likely, it behooves defense counsel to “get in early” to the government. Counsel should aim to negotiate a guilty plea agreement, including sentencing guideline offense characteristics like fraud loss, before what is readily provable hardens into evidence that the prosecutor may not ignore based on the government’s continuing investigation. The dilemma, of course, is that sometimes it is difficult to assess the risk of indictment and conviction in the early stages of a government investigation.

For potential white collar defendants, the conditions for a perfect storm exist: heightened public attention, stiffer and more expansive criminal laws, more severe sentencing guidelines, more stringent appellate review, and the Department of Justice emphasizing a “get tough” attitude through its practices and policies.

\textsuperscript{160} See, e.g., \textit{United States v. Thurston}, 338 F.3d 50 (1st Cir. 2003) (reversing a downward departure to healthcare fraud defendant that had been granted on grounds including extraordinary charitable and community service).
\textsuperscript{161} 18 U.S.C. § 3742(e)(3)(C). Although a complex issue that is not yet resolved, defense counsel should also consider the \textit{ex post facto} implications of this new appellate standard of review, which arguably reduces the government’s burden.
\textsuperscript{162} Memorandum from Attorney General Ashcroft, \textit{Department Policy Concerning Charging Criminal Offenses, Disposition of Charges, and Sentencing} (Sept. 22, 2003).
\textsuperscript{163} Memorandum from Attorney General Ashcroft, \textit{Department Policies and Procedures Concerning Sentencing Recommendations and Sentencing Appeals} (July 28, 2003).
V. IMPACT OF SOA ON ORGANIZATIONS

A. Prosecuting Organizations

The SOA §§ 302 and 906 certification provisions target CEOs and CFOs. Yet, as we all know from the *Arthur Andersen* prosecution,\(^{164}\) organizations as entities are also subject to prosecution and sentencing for financial and accounting fraud and related obstructions of justice. It is likely that any investigation that develops evidence of a CEO's or CFO's violation of SOA § 906 will also be one in which that CEO's or CFO's corporation has exposure under the fraud laws.

Whether or not a corporation will be charged federally is a judgment call ultimately made by the prosecutor. Federal prosecutors are to be guided in this decision by the DOJ's recently revised policy directive on “Federal Prosecution of Business Organizations.”\(^{165}\) This policy lists and explains nine factors that are to go into the decision of whether or not to charge a corporation:

1. the nature and seriousness of the offense,
2. the pervasiveness of the wrongdoing within the corporation,
3. history of similar conduct including prior criminal, civil or regulatory actions,
4. timely and voluntary disclosure of wrongdoing to, and cooperation with, the government,
5. the adequacy of the corporation’s compliance program,
6. the corporation’s remedial actions,
7. collateral consequences of prosecution, *e.g.*, to employees,
8. the adequacy of individual prosecutions, and
9. the adequacy of civil or regulatory remedies.\(^{166}\)

Two points stand out in this list. First, the government expects voluntary disclosure and cooperation. Moreover, the government defines cooperation to include “if necessary, waiver of attorney-client and work product protection” as to “the factual internal investigation and any contemporaneous advice given to the corporation concerning the conduct at issue.”\(^{167}\) While the government does not consider such a waiver to be an “absolute requirement” of cooperation, it is “one factor in evaluating the corporation’s

---


\(^{166}\) *Id.* at § II (A).

\(^{167}\) *Id.* at §§ II(A)(6), VI(B) n.3.
cooperation” and thus in deciding whether to charge the entity.\textsuperscript{168} Another factor in the government’s evaluation of cooperation is whether or not the company is indemnifying target individuals or is otherwise seen to be protecting culpable employees.\textsuperscript{169}

Second, the existence and adequacy of a corporate compliance plan is essential. The DOJ policy cites the \textit{Caremark} case and goes on to comment:

Prosecutors should . . . attempt to determine whether a corporation’s compliance program is merely a “paper program” or whether it was designed and implemented in an effective manner . . . . [P]rosecutors should determine whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation’s compliance effort. In addition, prosecutors should determine whether the corporation’s employees are adequately informed about the compliance program and are convinced of the corporation’s commitment to it.\textsuperscript{170}

Compliance plans neither legally absolve the corporation of criminal liability under the doctrine of \textit{respondeat superior} nor guarantee immunity from prosecution. However, as a DOJ official stated recently, a company that does not have a compliance program is “a little like conducting your business without insurance.”\textsuperscript{171} Compliance plans are discussed in detail below.

\section*{B. Sentencing Organizations}

The sentencing of corporations and other entities is governed by the federal sentencing guidelines.\textsuperscript{172} The express purpose of the “organizational guidelines” is “to provide just punishment, adequate deterrence, and incentives for organizations to maintain internal mechanisms for preventing, detecting, and reporting criminal conduct.”\textsuperscript{173}

For fraud offenses, the sentencing court is to calculate the offense level as it would for an individual defendant.\textsuperscript{174} A “base fine” would then be the greater of that called for by this offense level calculation, the pecuniary gain to the organization, or the pecuniary loss caused by the offense.\textsuperscript{175} A “culpability score” based on aggravating and mitigating

\begin{thebibliography}{99}
\bibitem{168} \textit{Id.} at § VI(B); \textit{see infra} footnote 183 regarding recommendations from the Ad Hoc Advisory Group on the Organizational Guidelines concerning the impact of a failure to waive privileges on downward departures from the sentencing guidelines.
\bibitem{169} \textit{Id.} at §VI(B). Obviously, some states by law require corporations to pay the legal fees of officers and directors prior to a formal determination of guilt. Compliance with such laws is not to be considered a failure to cooperate. \textit{Id.} at n.4.
\bibitem{170} \textit{Id.} at § VII(B).
\bibitem{172} U.S.S.G., Ch. 8 (eff. Nov. 1, 2002).
\bibitem{173} \textit{Id.} at Ch. 8, Introductory Commentary.
\bibitem{174} U.S.S.G. §§ 8C2.1(a), 8C2.3 (eff. Nov. 1, 2002).
\bibitem{175} U.S.S.G. § 8C2.4 (eff. Nov. 1, 2002).
\end{thebibliography}
factors is then calculated in order to find “multipliers” to be applied to the base fine to generate the minimum and maximum of the guideline fine range.\textsuperscript{176}

Of note is that this culpability score is reduced if the defendant corporation had in place an “effective program to prevent and detect violations of law” so long as high-level or compliance personnel were not involved in the charged offense and the corporation did not unreasonably delay reporting the offense to the government.\textsuperscript{177} An “effective program to prevent and detect violations of the law” requires “at a minimum” that the organization exercise due diligence by taking the following steps:

1. establish compliance standards and procedures,
2. assign high-level personnel to oversee compliance,
3. ensure that discretionary authority is not delegated to individuals with a propensity for illegal activity (background screening),
4. effectively communicate to employees about compliance standards and procedures (training),
5. take reasonable steps to ensure compliance with standards through monitoring, auditing and reporting systems,
6. adequately and consistently enforce standards, including, as appropriate, discipline for offenders, and
7. respond to infractions and take steps to prevent subsequent occurrences.\textsuperscript{178}

The guidelines recognize that “one size does not fit all” when developing a compliance program. “The precise actions necessary for an effective program” will depend on factors including the size of the organization, the risks attendant to the particular nature of the business, the organization’s history, and applicable industry practice and government regulation.\textsuperscript{179}

Further culpability score reductions are available for corporate self-reporting, cooperation, and acceptance of responsibility.\textsuperscript{180} In addition, a corporation may receive a downward departure from its guideline fine range, on government motion, if the corporation provides “substantial assistance in the investigation or prosecution” of another organization or an unaffiliated individual.\textsuperscript{181}

Conversely, as a condition of probation for recidivist entities or those without compliance plans, the court may order the entity to develop and submit to the court a

\textsuperscript{176} U.S.S.G. §§ 8C2.5-8C2.8 (eff. Nov. 1, 2002).
\textsuperscript{177} U.S.S.G. § 8C2.5(f) (eff. Nov. 1, 2002).
\textsuperscript{178} U.S.S.G. § 8A1.2, App. Note 3(k)(1)-(7). These principles have become the foundation for the OIG Compliance Guidance issued for various types of healthcare providers.
\textsuperscript{179} Id. at App. Note 3(k)(i)-(iii).
\textsuperscript{180} U.S.S.G. § 8C2.5(g) (eff. Nov. 1, 2002).
\textsuperscript{181} U.S.S.G. § 8C4.1 (eff. Nov. 1, 2002).
program to prevent and detect violations of law, including a schedule for implementation, communication to employees and shareholders, and unannounced site inspections.\textsuperscript{182}

This emphasis on corporate compliance programs both in DOJ prosecution policy and in the federal sentencing guidelines will not likely abate. Indeed, an \textit{ad hoc} advisory group to the federal Sentencing Commission recently issued a report recommending, among other things, a separate guideline to define with more precision the components of an “effective” compliance program, with an emphasis on organizational culture, leadership responsibilities, compliance staff and resources, training and periodic evaluation, and ongoing risk assessment.\textsuperscript{183}

\section*{C. Impact on Privately Held and Not-For-Profit Healthcare Organizations}

It is difficult to imagine a scenario in which privately held and not-for-profit healthcare companies will not be touched by SOA and its ripple effects. Indeed, some clients report that it has already done so. As noted above, some SOA provisions, such as those having to do with document destruction and whistleblower retaliation, do directly affect privately held companies. While the SOA certification provisions discussed in this paper do not directly apply, it seems inevitable that pressure for due diligence, if not outright certification, will result in similar obligations in the private sphere. The pressure is likely to come from a variety of sources:

- Board members more than ever are aware of their own potential exposures. As a result, there is a top down push on CEOs and CFOs for internal compliance regimes and certifications.

- State attorneys general and legislatures are recognizing that the public policies served by the SOA apply to all organizations, whether they are profit-driven or mission-driven. The AHERF collapse stands as a cautionary example. State attorneys general usually have jurisdiction over not-for-profit organizations, and it would not be surprising to see annual filing requirements enhanced at their urging.

- Bond dealers, investment banks, lenders, and bond rating services are demanding that SOA-type standards be put in place to protect and to help accurately gauge the risk of investments.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{182} U.S.S.G. § 8D1.4(c) (eff. Nov. 1, 2002).
\item \textsuperscript{183} Report of the Ad Hoc Advisory Group on the Organizational Guidelines (Oct. 7, 2003), available at: www.uscc.gov/corp/advgrp/advgrp.htm. The \textit{ad hoc} group also recommends that the waiver of privilege and work product protection as part of a corporation’s cooperation with the government not be an absolute prerequisite for a culpability score reduction and encourages further dialogue on the so-called “litigation dilemma,” \textit{i.e.}, truly effective compliance programs increase the risk that the information generated by the program will be used by potential litigants to harm the organization.
\end{itemize}
\end{footnotesize}
• Underwriting requirements from Directors and Officers (D&O) liability insurers are becoming more demanding and tracking SOA standards in order to minimize insurers’ risk of exposure.

• Auditors are seeking more stringent SOA-related representations and warranties from management in order to limit their gatekeeper liability.

• A sensitized IRS\textsuperscript{184} likely will be looking to more strictly enforce intermediate sanctions\textsuperscript{185} in order to hold tax exempt organizations to SOA-type standards of behavior.

\textsuperscript{184} The IRS Exempt Organizations Office reportedly intends to increase its enforcement presence via a new compliance unit used to review the Form 990 informational returns of tax-exempt entities. Intermediate sanctions in connection with excessive compensation packages are also said to be of concern. See IRS Exempt Organizations Office To Boost Compliance Efforts in 2004, 8 BNA HEALTH CARE DAILY REPORT 241, Dec. 16, 2003.

\textsuperscript{185} 26 U.S.C. § 4958.
VI. COMPLIANCE IMPLICATIONS

A. SOA Mandates Internal Controls Over "Disclosure" and "Financial Reporting"

As discussed above, per the June 2003 amendments to the § 302 certification requirements, CEOs and CFOs now must certify that they are responsible for designing and maintaining (or delegating responsibility for designing and maintaining) two kinds of internal controls.

First, they must acknowledge responsibility for "disclosure controls and procedures," which are defined as "controls and other procedures of an issuer that are designed to ensure that information required to be disclosed by the issuer [in its periodic reports] is recorded, processed, summarized and reported, within the time periods" specified for the filing of those reports. These "disclosure controls" address both financial and non-financial information that is included in a company's periodic reports. The SEC left the particular requirements for establishing and evaluating these controls to each filing company: "we expect each issuer to develop a process that is consistent with its business and internal management and supervisory practices." However, the Commission recommended that companies create a committee that would be charged with considering the materiality of information and determining the company's resulting disclosure obligations.

Signing officers must also certify that they are responsible for establishing and maintaining "internal control over financial reporting" for their companies. This term is defined as

a process defined by, or under the supervision of, the issuer’s principal executive and principal financial officers . . . effected by the issuer's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles.

It includes procedures regarding the maintenance of reasonably detailed records regarding assets and transactions, the approval or authorization of receipts and expenditures, and means to prevent or detect any unauthorized acquisition, use, or

---

186 See, e.g., 17 C.F.R. § 240.15d-14(c). Per 17 C.F.R. § 240.15d-15, the SEC requires every issuer that files periodic reports to maintain these disclosure controls and procedures. Moreover, those controls and procedures must be evaluated at the end of each fiscal quarter, in a manner than involves the company's CEO and CFO. Similar obligations arise under Exchange Act Rules 13a-14 and 13a-15. See 17 C.F.R. §§ 240.13a-14; 240.13a-15.
188 See id.
disposition of the issuer’s assets that could have a material effect on the financial statements.\textsuperscript{190}

These SOA provisions effectively mandate at least some form of compliance program with respect to publicly held companies' SEC reporting requirements. For healthcare companies, which have been urged for years by the Office of Inspector General for the Department of Health and Human Services (OIG-HHS) to adopt compliance programs that will ensure regulatory compliance, the SOA requirements may either speed up implementation of a comprehensive compliance program or expand existing efforts to ensure compliance. Indeed, while the SOA requirement for "internal controls over financial reporting" may be limited to accounting measures, the broader requirement for "disclosure controls" necessarily implicates regulatory and other forms of compliance. In addition, other SOA provisions reinforce the notion that a comprehensive compliance program is now required by law. For example, in the regulations adopted under § 406 of the Act, companies must disclose whether or not they have adopted a code of ethics for senior officers—and if not, companies must explain why such a code has not been adopted.\textsuperscript{191}

Thus, under the SOA, a compliance program is required for all publicly traded companies. For businesses that are involved in highly regulated areas, such as healthcare, a compliance program is essential for both public and private companies, and should be comprehensive in scope (i.e., it should address all areas of potential legal risk). Because healthcare providers, like all companies, can vary widely in terms of size, complexity, mission, and corporate culture, a compliance program should be specifically designed to meet the needs of the particular company.

\textbf{B. The Challenge for Privately Held and Not-For-Profit Organizations}

The challenge for privately held organizations will be twofold. First, management-board relations must be structured so that board members have a role in ensuring the integrity of internal reporting systems but retain sufficient distance to help direct the overall strategic direction of the entity. Board members cannot become micro-managers or auditors.\textsuperscript{192} Second, management must develop methods to demonstrate and document its due diligence in assuring that these reporting systems have integrity and that related reports and certifications are accurate and fair.

For the board, or its audit committee, this means developing a clear understanding, in writing, of board members' roles. It also means creating direct lines of communication with key players such as the compliance officer and auditor so that pertinent oversight questions can be put directly to the responsible individual. Finally, it is worth considering whether the board should develop a list of oversight questions, financial or otherwise, to

\begin{itemize}
\item \textsuperscript{190} Id., amended 17 C.F.R. § 240.13a-15.
\item \textsuperscript{192} This tension in the board’s role can be encapsulated by the acronyms NIFO (“nose in, fingers out”) or BIGO (“be Involved, but get out of the way”).
\end{itemize}
help frame its inquiries of management as matters are presented or as “red flags” appear.

For top management, the challenge is to demonstrate and document good faith in its reporting process. This means laying out a due diligence process, which might include reviewing draft and final versions of reports; meeting with top financial and operational officers to understand the process by which the report is produced and to get at the assumptions and judgment calls underlying the report; meeting with those responsible for key functions and major business units to gauge whether the results of operations are being fairly presented; and participating in discussions with auditors and the board audit committee regarding tough issues, close calls, problem resolution and any matters that were omitted in the preparation of a report.

C. Creating an Effective Compliance Program

Many healthcare providers have heeded the advice and guidance of the OIG-HHS and adopted compliance programs that are tailored to address the risks that their particular business is likely to face. For these businesses, adopting measures to ensure compliance with Sarbanes-Oxley should be relatively easier.

As a general rule, a company’s compliance program should include the seven elements that are listed in the U.S. Sentencing Guidelines as indicators of an effective compliance program. The program should:

1. Have in place written standards and procedures to be followed by the company’s employees and other agents that are reasonably capable of reducing the prospect of criminal conduct;

2. Assign to specific, high-level individuals within the organization the responsibility to oversee compliance with the company’s standards and procedures;\textsuperscript{193}

3. Have in place a system for appropriate background and program exclusion checks. That is, use due care not to delegate substantial discretionary authority to individuals whom the company knows, or should know, have a propensity to engage in illegal activities;

4. Take reasonable steps to communicate effectively the company’s standards and procedures to all employees and other agents by, for example, requiring participation in training programs or disseminating publications that explain in clear and practical terms what the company’s policies and procedures require;

\textsuperscript{193} The idea of creating a “business practice officer” (BPO), or private inspector general, within the corporation is not a new one. As conceived by some, the BPO would be independent of management, assist in the establishment of standards, monitor and help enforce those standards, report to the board audit committee and/or independent members of the board, and, possibly, even report directly to shareholders. \textit{See}, e.g., Hon. Stanley Sporkin, Remarks before the Business Week Conference of Corporate Directors, McGraw Hill, New York (June 16, 1978).
5. Take reasonable steps to achieve compliance with the company’s standards by, for example, using monitoring and auditing systems designed to detect criminal conduct by company employees and by having a reporting system in place where employees and others can notify the company of criminal conduct by others within the organization without fear of retribution;

6. Consistently enforce the company’s standards through appropriate disciplinary mechanisms, including the appropriate discipline of employees responsible for failing to detect an offense; and

7. Take all reasonable steps to respond appropriately to offenses that are detected and to prevent further similar offenses, including any necessary modifications to the company’s compliance program to detect and prevent violations of law.\textsuperscript{194}

These factors apply equally to financial and disclosure reporting compliance policies and procedures.

At a bare minimum, companies that are subject to the SOA and its regulations must adopt a code of ethics that applies to its senior financial officers and its principal executive officer. Pursuant to § 406 of the SOA, the SEC has defined "code of conduct" to mean written standards that are "reasonably designed to deter wrongdoing" and promote:

- Honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships;

- Full, fair, accurate, timely, and understandable disclosure in reports and documents that a registrant files with, or submits to, the Commission and in other public communications made by the registrant;

- Compliance with applicable governmental laws, rules, and regulations;

- The prompt internal reporting to an appropriate person or persons identified in the code of violations of the code; and

- Accountability for adherence to the code.\textsuperscript{195}

The regulations require companies to disclose whether they have adopted such a code of conduct, and if not, to provide an explanation. Moreover, the regulations mandate that companies make their code of conduct available for public inspection.\textsuperscript{196} While the SEC commented that companies may choose to have a code of ethics that applies only


\textsuperscript{196} See id.
companies to adopt codes that are broader and more comprehensive than necessary to meet the new disclosure requirements." Finally, the SEC does not prescribe internal enforcement measures, but hints that companies should adopt appropriate measures to ensure compliance with the code of ethics.

As a practical matter, a code of ethics is just the first step in creating a comprehensive compliance program that will protect both a company and its officers who must make certifications to the SEC and other government agencies. In devising an appropriate program, a company should consider the following.

1. **What are the company’s potential areas of risk?**

The first step in customizing a compliance program is to evaluate those areas where the company is subject to laws and regulations, some of which can be very detailed and not necessarily intuitive from a business perspective. Healthcare providers can begin this analysis by reviewing the compliance guidances, tailored to particular industry groups that have been issued by OIG-DHHS over the past few years. The guidances uniformly incorporate the seven elements that are recognized in the U.S. Sentencing Guidelines as indicators of an effective compliance program.

Beyond the OIG-DHHS compliance guidance, a company should consider what other laws and regulations apply to its business, including:

- Medicare and other federal healthcare program regulations
- Food and Drug Administration regulations
- Anti-kickback and physician self-referral provisions
- Privacy law (e.g., HIPAA) issues
- Securities laws
- Employment issues, including workplace safety laws and anti-retaliation statutes
- Environmental laws and regulations
- Export control laws
- Anti-trust laws
- Anti-terrorism laws
- Anti-money laundering laws
- Internal Revenue laws (e.g., intermediate sanctions)
- State law issues (e.g., licensing)

Once these areas of potential risk are identified, compliance efforts can focus on education, training, and reporting mechanisms, as well as on the development of strategies for preventing and responding to problems that may arise.

---

197 *Id.*

2. **How can the company disseminate information to those who need it?**

Education and training are vital tools in establishing an effective compliance program. The SOA requires disclosure of whether a code of ethics for senior financial officers has been promulgated. However, any company—Enron, for just one example—can draft a code of conduct and policies and procedures. Unless the company’s management and employees understand the purpose of the company’s rules (i.e., how they are connected to laws and regulations) and can identify when the company’s policies are being violated or are at risk, compliance cannot work.

Compliance training tools have become fairly sophisticated and flexible, and a variety of computer and web-based programs can be customized to a company’s particular needs. These tools can be particularly effective for healthcare companies that have employees working shifts, that are trying to create a consistent compliance atmosphere across a number of geographically dispersed locations, or in businesses that experience high rates of turnover. Computer-based training permits employees to attend training at their convenience (preferably at the beginning of their employment and periodically thereafter), and allows the employer to keep track and run reports of who has received training.

3. **What mechanisms are in place to ensure that information is being reported to those who need to know and can react to it?**

Of particular importance to CEOs and CFOs who must attest to the SOA certifications is ensuring that information within the company is promptly reported to management so that any problems or issues can be addressed—and, if required, properly disclosed in the company’s periodic reports to the SEC. In addition, both inside and outside counsel should be attuned to their SOA obligations to report material violations of the securities laws, breaches of fiduciary duty, or similar violations “up-the-ladder” within the company.

The SOA requires audit committees to establish procedures for the anonymous reporting of complaints regarding accounting and auditing matters. In the context of healthcare compliance programs, the OIG-HHS recommends establishing a telephone hotline that employees at all levels can use to report problems anonymously.

Whatever method of reporting is instituted should provide reporting employees

---

201 Section 10A(m), Securities Exchange Act of 1934 (SOA § 301).
assurances of anonymity, non-retaliation, and a means for finding out, in some appropriately limited or general way, what steps the company has taken in response to the report. 203

In addition to creating an anonymous reporting method, corporate officers and directors subject to SOA requirements may also wish to seek affirmative assurances from their subordinates that confirm appropriate disclosures and behavior at all levels of the company. In essence, the company may wish to establish internal certification requirements on which the CEO and CFO can then rely in making the required certifications to the SEC.

Another key component in ensuring compliance is the establishment of regular and periodic compliance audits and reviews of the company’s risk areas. Depending upon the scope of the review, these periodic audits can be conducted internally or may be more appropriately run by outside consultants or auditors. In addition to confirming that the company’s reporting mechanisms are functioning properly, an external review and audit can reveal issues that have escaped notice, because they involve problematic practices that unintentionally have become accepted ways of doing business. 204

Importantly, under the SOA certification, the CEO and CFO must attest that they have evaluated the effectiveness of the company’s disclosure controls and procedures themselves, as well as the company’s internal controls over financial reporting. They must also attest that they have disclosed their conclusions about these internal controls and any changes or significant deficiencies in these controls in the company’s reports to the SEC and, with respect to financial reporting, to the audit committee of the board of directors. 205 In effect, the certification requirement establishes a mandatory periodic review of a company’s overall compliance program.

Additionally, beginning in 2004, companies will need to include in their annual reports to the SEC a copy of their registered public accounting firm’s attestation report on management’s assessment of internal controls. 206 This rule only confirms that the SEC is looking for detailed, thorough reviews of the company’s controls and procedures, as an assurance of their effectiveness.

203 It is widely believed that employees who report problems and who perceive them not to have been investigated or acted upon by the company are more likely to take their concerns directly to the government. The SOA, like other federal statutes that impact on healthcare providers, contains strict anti-retaliation provisions that protect whistleblowers. Healthcare counsel should note that the SOA whistleblower protection statute is very broad. Applicable to actions committed after July 30, 2002, it reaches any harmful action targeting any person who provides any quantum of truthful information to law enforcement about the possible commission of any federal crime. 18 U.S.C. § 1513(e) (SOA § 1107); see also 18 U.S.C. § 1514A (SOA § 806 - civil whistleblower protection statute).

204 A compliance audit is different, and perhaps broader, than a financial audit. It is a review of the company’s adherence to its own policies and procedures as well as its compliance with applicable laws and regulations.

205 See 68 Fed. Reg. 36,635 (June 18, 2003). This same rulemaking announced that such evaluations of a company’s disclosure controls and procedures must be made at the end of the reporting period.

206 See id.
Both internal reporting mechanisms and periodic review processes should be well-documented so that, if an issue does arise, or if the government decides to investigate, the company will have a tangible audit trail to demonstrate its compliance efforts.

4. Does the company have policies and procedures in place to address problems that may arise, and is action in fact taken when an issue is discovered?

It is not enough that a company monitor and report issues that may arise within its organization; under the Sentencing Guidelines factors, an effective compliance plan will also address those issues to correct and prevent the problem from recurring. A typical first step, based upon the nature and severity of the issue that has come to light, may be to conduct an internal investigation to verify the existence of the problem and determine its scope. Matters that raise serious legal issues, such as employee fraud or misconduct by high level personnel, should, at a minimum, be referred to inside legal counsel for review. To preserve privileges and protections, and to avoid conflicts of interest, it may be wise to employ outside counsel to conduct the review.

Employees throughout the company should be aware that breaches of the company's policies, including policies to comply with applicable laws and regulations, can and will result in disciplinary measures, up to and including termination (depending upon the severity of the violation). Merely stating this policy is not sufficient; if the company's compliance program ever comes under scrutiny by the government, the company should be able to demonstrate that it has taken appropriate measures to discipline and correct problems when they arise. Again, documentation of these efforts is important to support the company's assertion that it maintains an effective compliance program.207

For certain kinds of healthcare,208 securities209 or other violations (e.g., for what may reasonably appear to be an intentional violation of regulations related to federal healthcare programs), the company may choose to make a voluntary “self-disclosure” to the government and resolve any liabilities before the issue is affirmatively discovered or investigated as a serious fraud or other matter. This, and other attempts to resolve issues that may involve negotiations with a government agency charged with overseeing the company's adherence to applicable laws and regulations, should be discussed with outside counsel.

207 The need for documentation has been specifically clarified by the SEC: “[W]e believe that it should have been clear previously that documentation of internal controls is also required. In case it wasn’t, the [§ 404] release reiterates that documenting controls is a management responsibility.” Remarks of Scott A. Traub, Deputy Chief Accountant, SEC, available at: www.sec.gov/news/speech/spch052903sat.htm. (emphasis in original).


5. Has company management emphasized compliance in such a manner as to infuse the corporate culture with a sense that ethical behavior is rewarded?

Finally, it is important to bear in mind that the overall objective of the SOA is to reinforce the ethos that corporate America conduct its business in a manner that is both legally and ethically appropriate. Federal enforcement agencies (DOJ, OIG-DHHS, and others) have, over the years, seen a multitude of approaches to compliance. They seek to assess and conclude whether a company’s efforts at compliance are taken seriously by management and incorporated into the corporate culture or are mere “paper” programs. While a detailed program of compliance may address the Sentencing Guidelines requirements and appear comprehensive on paper, in the current enforcement climate, the government ultimately is looking to see whether the company is actually impressing upon its employees the obligation to "do the right thing," regardless of specific written protocols.

That message of ethical behavior must be initiated at the highest levels of the organization. Congress's demand that CEOs and CFOs personally certify the company's periodic reports to the SEC embodies this notion. Officers and directors of the company should be vigilant in emphasizing the need to comply with laws and regulations, not just as a means of avoiding liability, but as the only way to conduct business in a post-SOA world.
VII. CONCLUSION

Healthcare lawyers are accustomed to the challenges posed by the regulatory framework of Medicare and Medicaid and related administrative, civil and criminal enforcement statutes and regulations. The corporate governance spotlight illuminates a whole other layer of risk and exposure. The prosecution of violations of fraud, false statement and certification statutes now may reach to the upper spheres of management and even to the board. Moreover, governance failures may also spill back over more traditional healthcare compliance laws, such as the Anti-Kickback and False Claims Acts, to create the evidence of intent necessary to prosecute under those statutes as well.