Corporate Monitors: How to Avoid One If Possible and How to Deal With One If You Must

By John F. Wood

Over the past 15 years, independent compliance monitors have become increasingly common in Department of Justice (DOJ) resolutions of enforcement matters with corporations. Now, other federal agencies, state attorneys general, and even foreign government enforcement agencies are beginning to require monitors as well. This trend serves only to increase the need for corporate executives to understand the corporate monitor phenomenon and how imposition of a monitor could affect their companies.

This article addresses several issues that should be at the top of corporate executives' minds regarding monitorships—for example, what are the roles and responsibilities of a monitor, what steps a company can take to help avoid having a monitor imposed in the first place, how to work with a monitor if one is appointed, and whether there is a risk that the monitors' reports will become public.

What Is an Independent Compliance Monitor?

Independent compliance monitors were used rarely prior to the corporate scandals of 2001 and 2002. But following the scandals of Enron, WorldCom, Arthur Andersen, and other companies, corporate criminal prosecutions became a much higher priority for DOJ. The high-water mark for corporate prosecutions was DOJ's decision to seek and obtain an indictment of Arthur Andersen, which led to the demise of the venerable accounting firm. The fall of Arthur Andersen, in turn, led to a more concerted effort by DOJ to utilize (when possible) means of punishing corporations that were less drastic than indictment. Accordingly, DOJ increasingly relied on deferred prosecution agreements and non-prosecution agreements. Under these agreements, DOJ would agree not to move forward with a case against the company if the company agreed to certain actions, which usually involve paying a hefty fine, taking remedial actions, enhancing the company's compliance program, and preventing recurrence of the misconduct for some defined

© 2017 Hughes Hubbard & Reed LLP. *John F. Wood is a Partner of Hughes Hubbard & Reed LLP. John served in numerous high-level executive branch positions, including U.S. Attorney for the Western District of Missouri, Chief of Staff for the U.S. Department of Homeland Security, Deputy Associate Attorney General, Counselor to the U.S. Attorney General, and Deputy General Counsel for the White House Office of Management and Budget.*

the Corporate Governance advisor

Copyright © 2017 CCH Incorporated. All Rights Reserved.

The ***CORPORATE GOVERNANCE ADVISOR*** (ISSN 1067-6171) is published bimonthly by Wolters Kluwer at 76 Ninth Avenue, New York, NY 10011. Subscription rate, $895 for one year. POSTMASTER: Send address changes to *THE CORPORATE GOVERNANCE ADVISOR,* Wolters Kluwer, 7201 McKinney Circle, Frederick, MD 21704. Send editorial correspondence to Wolters Kluwer, 76 Ninth Avenue, New York, NY 10011. To subscribe, call 1-800-638-8437. For Customer service, call 1-800-234-1660. This material may not be used, published, broadcast, rewritten, copied, redistributed or used to create any derivative works without prior written permission from the publisher.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other professional assistance is required, the services of a competent professional person should be sought.

—From a Declaration of Principles jointly adopted by a committee of the American Bar Association and a Committee of Publishers and Associations.

Permission requests: For information on how to obtain permission to reproduce content, please go to *www.WoltersKluwerLR.com/policies/permissions-reprints-and-licensing.*

Purchasing reprints: For customized article reprints, please contact *Wright's Media* at 1-877-652-5295 or go to the *Wright's Media* website *www.wrightsmedia.com.*

www.WoltersKluwerLR.com

period of time. Many of these agreements also included a provision requiring the appointment of a monitor. The monitor's role was to review the company's compliance with the terms of the agreement with DOJ for a defined period of time—usually two to four years (with three years being the most common).

The use of monitors quickly became controversial. Some of the early monitors were perceived as overly intrusive, with monitors reviewing day-to-day activities of the companies to seek out any evidence of further misconduct. Along with that broad monitor role came great expense, with some monitors costing companies tens of millions of dollars. The corporations subject to the monitors complained that they had too little say in the selection of the monitors, who were unilaterally chosen and imposed by DOJ. This concern took on greater prominence with the appointment of former Attorney General John Ashcroft to serve as monitor for Indiana-based medical supply company Zimmer Holdings. News reports indicated that Ashcroft's contract was worth between $28 million and $52 million, and his appointment as monitor by then U.S. Attorney Chris Christie led some to charge that DOJ was showing political favoritism in its appointment of monitors.

DOJ took much of the steam out of the criticisms by releasing in 2008 a set of principles to guide prosecutors in the selection and use of monitors. The principles explained that "[a] monitor's primary role is to evaluate whether a corporation has both adopted and effectively implemented ethics and compliance programs to address and reduce the risk of recurrence of the corporation's misconduct." The principles further called for companies to have a greater role in the selection of the monitors. Specifically, the principles stated that there should be a pool of three qualified candidates selected by the company, DOJ, or both, and that in many cases the company should submit its choice from among the three to DOJ for review and approval. Even in cases in which the selection process called for DOJ to play a greater role in selecting the monitor, the principles explain that DOJ should identify at least three acceptable monitor candidates and the company should choose from that list.

By making the monitor-selection process more competitive and giving the company greater say in the selection of monitors, DOJ has helped reduce the cost of monitorships, as monitor candidates now seek to be as cost-effective as possible in an attempt to be chosen for these prestigious assignments. Perhaps even more importantly, the role of the monitors has been clarified to some extent. Although every monitorship is different, today monitors tend to be less focused on monitoring the day-to-day activities of companies in search of evidence of misconduct, but instead tend to be more focused on reviewing the overall effectiveness of the companies' compliance programs as implemented. This is not to say that disputes among monitors and the companies they monitor have gone away, as there have been several recent disputes in which companies have complained that their monitors have run amok. But overall, monitors have become less costly and less intrusive since DOJ released its guidance principles.

Monitors are expected to review the companies' compliance programs (both on paper and in practice) and to assess the companies' adherence to their agreements with DOJ. In most cases, monitors are required to issue reports on a regular basis (often annually, but sometimes more frequently) to both the company and DOJ. Because the monitor is independent and not counsel to the company, these reports are not covered by the attorney-client privilege. They generally have been treated as confidential by both the companies and DOJ, but as explained later there have been recent efforts by the media and the public to obtain access to these reports.

Importantly, the DOJ principles apply only to DOJ-appointed monitors. As noted previously, many other enforcement agencies—including other federal and state agencies, as well as foreign government enforcement agencies—have begun requiring monitors as well. While in some cases those agencies look to DOJ's principles for guidance, often they do not. Perhaps the most

notable example is the New York Department of Financial Services, which has imposed monitors on several leading financial institutions that conduct business in New York.

Steps to Avoid the Appointment of a Monitor

Although monitorships have become less costly and less intrusive in recent years, the fact remains that no company has ever wanted to have a monitor imposed on it. There are several things that a company can do to reduce the chances of having a monitor imposed.

First, of course, a company should take steps to reduce the risk that it will violate the law at all. This requires having an effective compliance program, both on paper and in practice. The program should include strong policies and procedures, training, clear and compelling messages from company leadership about ethics and compliance, due diligence on business partners, and a strong internal compliance organization, among many other things.

Second, no compliance program is perfect, so even companies with the best of intentions might find themselves in the government's crosshairs. This is where the compliance program is critical once again. Even if the compliance program did not prevent all misconduct, DOJ might deem it sufficiently effective that an independent compliance monitor is not necessary. The most compelling issue for DOJ in determining whether to impose a monitor as a condition of settlement is whether DOJ has confidence in the company's compliance program to prevent a recurrence of the misconduct. If the compliance program is weak or still in development, DOJ is far more likely to require a monitor as a tool to help prevent and identify recidivism.

Third, some companies that are under investigation and fear that DOJ will appoint a monitor choose to proactively hire an outside law firm or investigative firm to serve as an independent compliance consultant. This is not a sure-fire way to head off the appointment of a monitor, but it may be seen by the government as a sign that the company has the matter under control. A self-imposed independent compliance consultant may be less intrusive and less expensive than an independent compliance monitor required by the government and reporting on a regular basis to the government.

How to Deal with a Monitor If You Must Have One

No company wants to have a monitor, but some are far worse than others. A good monitor can be relatively cost-effective, minimize disruption to business operations, and actually help make the company better in the long run. In contrast, a bad monitor can make corporate executives' lives miserable. So it is critical that the company get a monitor who understands the company's business realities and will seek to make the company better, rather than to make a name for the monitor or obtain a short-term windfall from the appointment. A company should consider not only a monitor candidate's credentials, but also the monitor's judgment, personality fit, and trustworthiness.

Once a monitor is in place, it is essential that the company be entirely honest and up front with the monitor. Even the most reasonable monitor will likely become intrusive if the monitor does not trust that the company is providing accurate and truthful information. Any effort to mislead the monitor or conceal information from the monitor will lead to distrust.

One of the best rules for dealing with a monitor is a "no surprises" rule. A good monitor will understand that no compliance program is perfect. When the inevitable shortcomings or mishaps occur, the company is far better off telling the monitor of the occurrence and how the company is addressing it than to have the monitor find out by other means. But this "no surprises" rule should run in both directions—the company should expect the monitor to inform the company of any shortcomings identified in the company's compliance program and give the company an opportunity to address

them, rather than play "gotcha" by raising the concerns for the first time in a report to the government.

With mutual trust and a constant flow of information between the monitor and the company, the monitorship can actually help make the company better suited for the future, while minimizing costs and intrusion on business operations.

Are Monitors' Reports Public?

As mentioned previously, the companies and DOJ generally treat monitors' reports as confidential, but there have been recent efforts by the media and the public to use the courts to gain access to these reports. The companies, DOJ, and the monitors themselves have all opposed such efforts to make the reports public. To date, two of these cases have reached the courts of appeals. In both cases the courts of appeals have concluded that the monitors' reports are not "judicial records," and therefore that the public does not have a First Amendment or common law right of access. But in some cases reporters have tried a separate route to get access to the reports—the Freedom of Information Act (FOIA). FOIA requires federal government agencies to produce certain records when requested by the public, but the law contains several exemptions. Thus far, DOJ has invoked FOIA's exemptions to avoid release of the monitor reports, but reporters have challenged DOJ's decision in court. Those cases are still being litigated, thus creating some remaining uncertainty about whether the reports could ultimately be released.

The possibility of public release of monitors' reports should cause great concern for the corporate community. Those reports often contain very sensitive business information, as a good monitor will explain in the reports how the program works in actual business contexts. If the reports were to become public, it could have a chilling effect on communications between companies and their monitors in the future. Companies might be reluctant to share sensitive business information with their monitors for fear that it could be included in the monitors' reports and ultimately released to the public. Likewise, a monitor who is sensitive to this concern might limit how much detail the monitor puts in the reports, which in turn can reduce the amount of information that the government obtains regarding the monitor's work.

The possibility that monitor reports could become public is all the more reason why companies should take steps proactively to make sure that they never have to have a monitor in the first place.