COSMOS
Navigate the Compliance Universe

CEP Magazine - November 2021
Should highly regulated public companies have board-level compliance committees?

By Paul E. Kalb, MD, andHolly J. Gregory

Paul E. Kalb (pkalb@sidley.com) heads the global Healthcare and FDA Group at Sidley Austin LLP. Holly J. Gregory (holly.gregory@sidley.com) is co-chair of Sidley Austin LLP's global Corporate Governance and Executive Compensation practice.

Directors are responsible for oversight of corporate compliance with legal and regulatory rules. In a series of recent cases, Delaware courts have clarified the circumstances in which directors may face personal liability if they fail properly either to implement or monitor their company's compliance.[1] The risk of such liability is heightened for directors of companies that face mission-critical risks, which can expose companies to significant criminal, civil, or administrative sanctions as well as harm to corporate operations and reputation. Such risks—arising, for example, under the False Claims Act; the Federal Food, Drug, and Cosmetic Act; the Foreign Corrupt Practices Act (FCPA); or Securities and Exchange Commission (SEC) rules—are particularly common in heavily regulated industries. The vast majority of public companies, however, including those in heavily regulated industries, do not have board committees dedicated to oversight of legal and regulatory risk. Boards that do not have such a committee should consider whether they should establish one to mitigate both corporate risk and risk to individual directors.

Directors have evolving duties to oversee compliance

Starting with the seminal decision in *In re Caremark Int'l Inc. Derivative Litig.* , the Delaware courts have made clear that board members have fiduciary obligations to oversee their company's compliance efforts. While plaintiffs seeking to impose personal liability on board members for violating these obligations face a high burden to bring such claims in shareholder derivative suits, the Delaware courts have emphasized that there are circumstances in which such claims are viable. The pace at which the courts have recognized such circumstances has accelerated over the past two years.

There are several key takeaways from these cases:

- Boards have responsibility not only to ensure that compliance systems are in place but also to monitor corporate compliance on an ongoing basis.[2] They must do so "rigorously" with respect to "mission critical" regulatory compliance risks.[3]
- When a compliance problem is brought to a board's attention, it cannot ignore the problem and should insist that appropriate action is taken.[4]
- Nominal compliance by *management* with regulatory rules does not, standing alone, satisfy the *board's* fiduciary oversight obligations.[5]
- A failure to satisfy these obligations may constitute a breach of the duty of good faith, an aspect of the duty of loyalty.[6] Though directors and officers insurance may financially protect directors in the event of a

breach of this duty, Delaware law does not allow companies to exculpate directors for a breach of the duty of loyalty or to indemnify directors for acts or failures to act that are not in good faith.[7]

- A factor in determining whether a company has established an adequate oversight mechanism is whether it has assigned a committee responsibility to oversee areas of critical risk;[8] an Audit Committee with a broad "risk compliance" mandate may not be sufficient.[9]