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

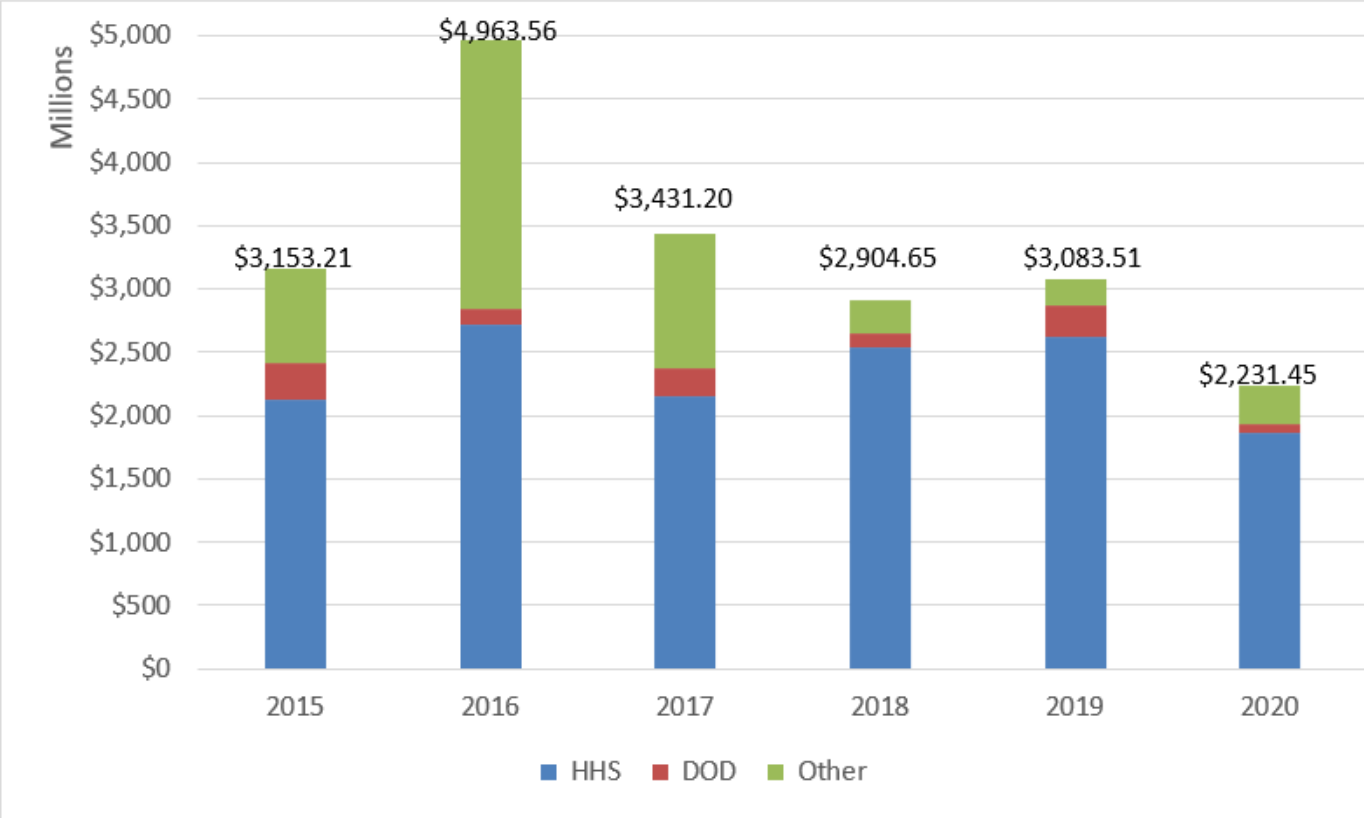
of loyalty.[6] Though directors and officers insurance may financially protect directors in the event of a breach of this duty, Delaware law does not allow companies to exculpate directors for a breach of the duty of loyalty or to indemnify directors for acts or failures to act that are not in good faith.[7]

- 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]

Regulatory risk in heavily regulated industries

Violations of legal and regulatory rules can be exceptionally costly for companies. Since 2015, for example, False Claims Act recoveries for healthcare companies totaled $14 billion, and recoveries in other industries, particularly the financial services industry, totaled another $5.7 billion (Figure 1).[10]

Figure 1: False Claims Act recoveries, 2015–2020



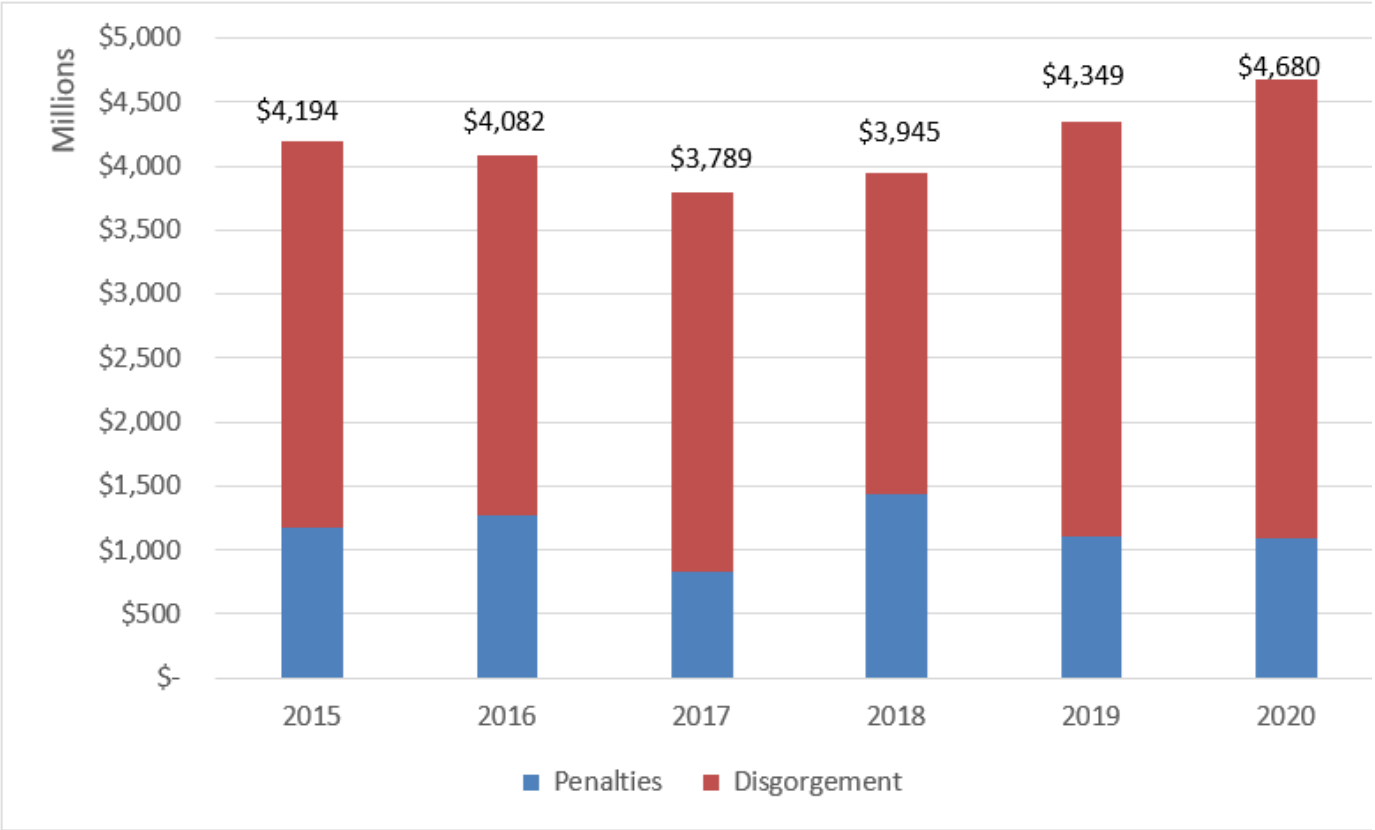
The percentage of healthcare-related recoveries has been particularly high in recent years. Despite the impact of the COVID-19 pandemic, the Department of Justice (DOJ) reported that it recovered more than $2.2 billion in False Claims Act settlements and judgments in 2020 and that almost $1.8 billion of those recoveries—more than 82%—came from the healthcare and life sciences industries.[11]

FCPA resolutions have increased substantially in recent years as well. Since 2000, FCPA resolutions have totaled over $18.2 billion in penalties, disgorgement, and prejudgment interest (Figure 2).[12] This staggering number does not include non-US fines, which can also be significant.

Figure 2: Corporate FCPA-related penalties, 2015–2020 (includes disgorgement; does not include non-US fi

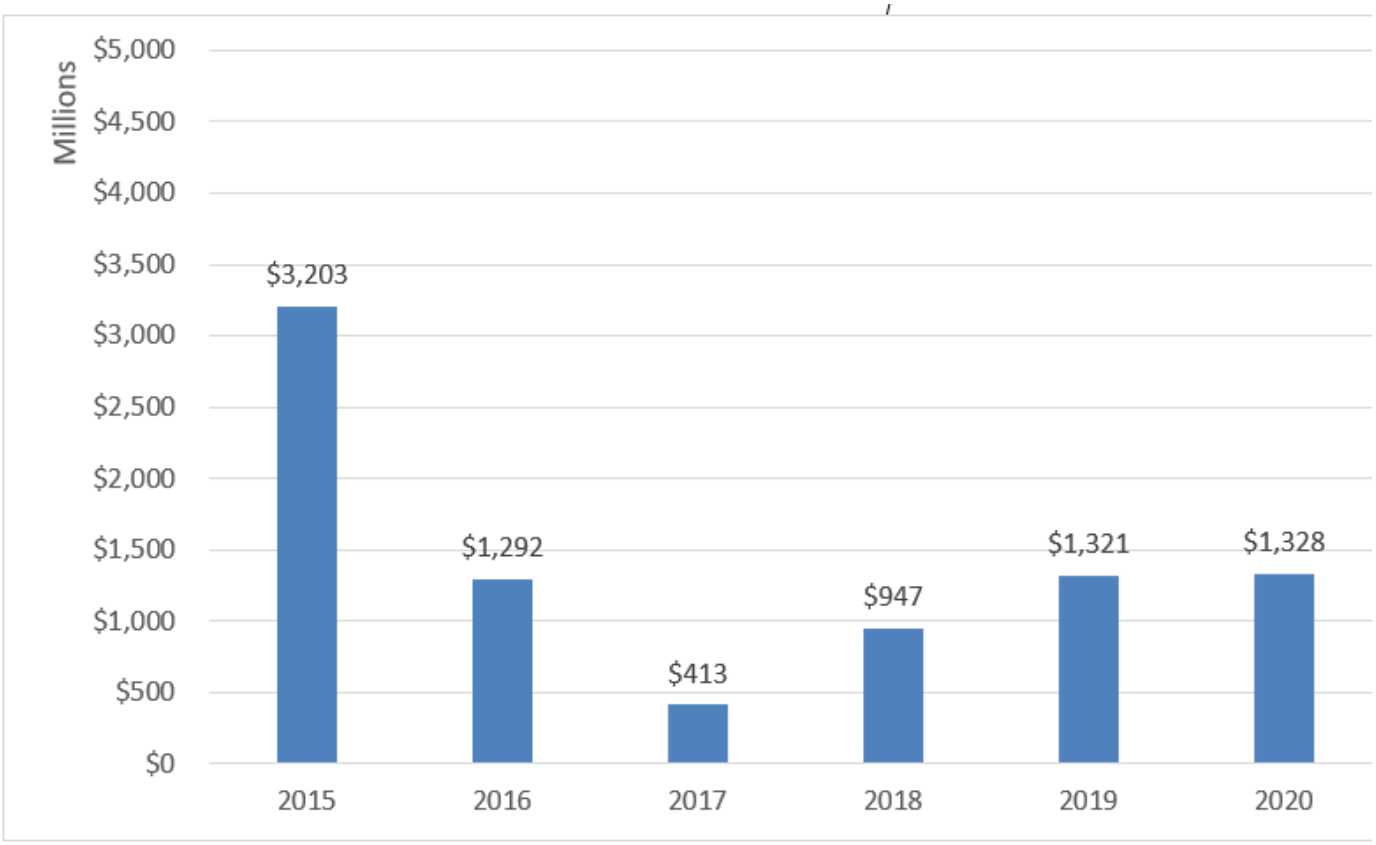
Other compliance-related regulation and enforcement is also on the rise, as both the SEC and Commodity Futures Trading Commission (CFTC) have contributed significant resources to pursuing compliance failures. Since 2015, the SEC has recovered more than $25 billion in penalties and disgorgement for compliance-related transgressions (Figure 3).[13]

Figure 3. SEC recoveries, 2015–2020



Similarly, since 2015, the CFTC has obtained orders imposing more than $8.5 billion in monetary relief as a result of its enforcement actions (Figure 4).[14]

Figure 4: CFTC recoveries, 2015–2020



Penalties for regulatory noncompliance are not limited to monetary fines. Compliance risk in heavily regulated industries can result in significant collateral consequences, including, but not limited to:

- Follow-on claims by other government agencies or private plaintiffs;
- Significant damage to reputation resulting in consumer distrust, increased government scrutiny, repeated investigations, and increased financial risk;
- Mandatory or permissive exclusion from participation in federal healthcare programs or suspension or debarment from government contracts;
- Individual or executive liability under the Department of Justice's Yates Memo[15] and subsequent directives requiring DOJ to hold individuals responsible for corporate fraud; and
- Individual liability under the Responsible Corporate Officer doctrine, also referred to as the *Park* doctrine, which permits the government to prosecute employees in a "position of authority" for failure to prevent or correct a violation of the Federal Food, Drug, and Cosmetic Act.[16]

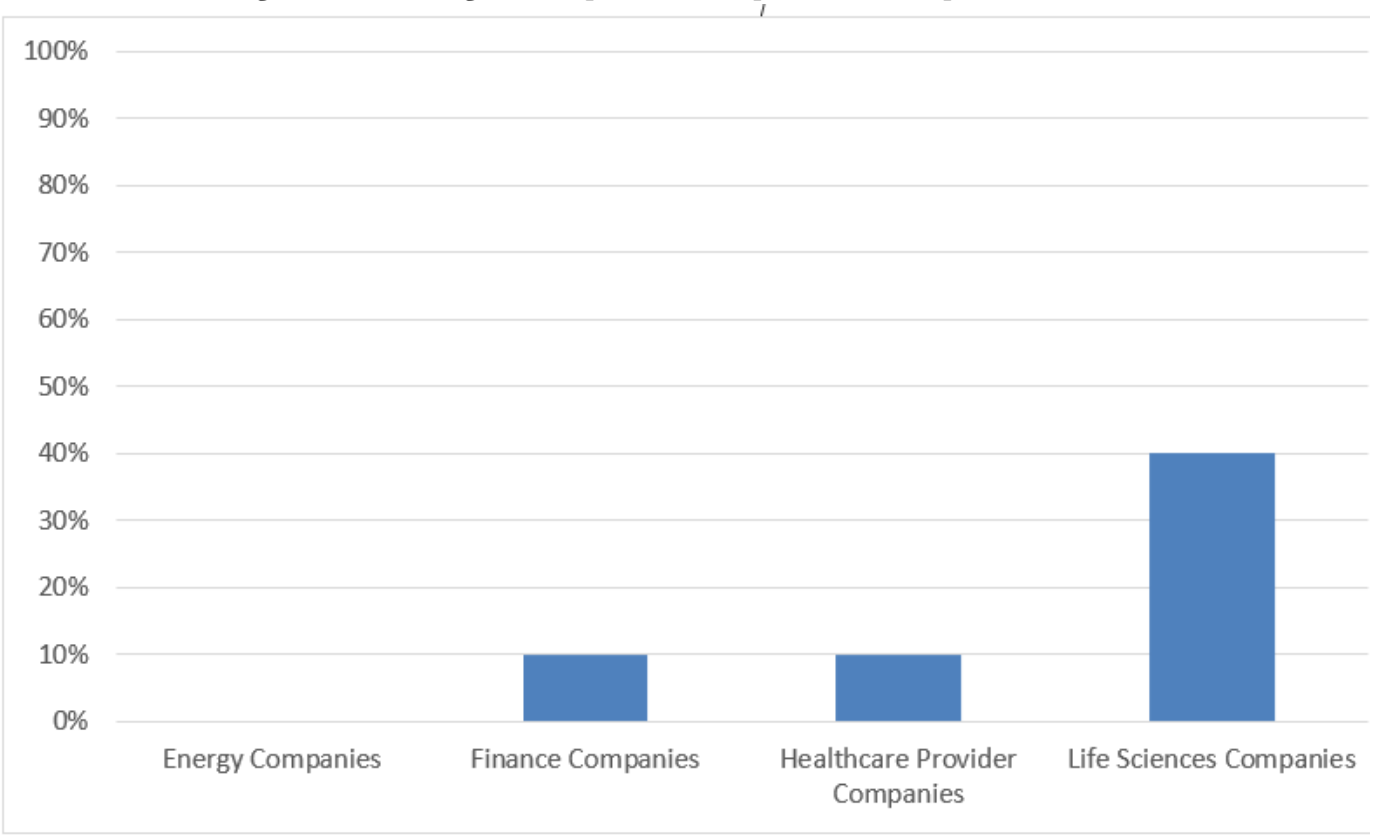
Overseeing compliance through audit committees

Notwithstanding the very substantial risks posed by regulatory noncompliance, the vast majority of boards do not have a committee focused principally or exclusively on oversight of their companies' regulatory compliance. A 2020 report, for example, found that 95% of S&P 500 companies delegate compliance oversight to a board committee that has other significant functions, such as an audit committee, while only 5% have established a specialized compliance-focused committee.[17] Similarly, Deloitte's 2018 *Board Practices Report* found that only

3% of boards surveyed reported having a standing compliance and ethics committee.[18]

Companies in at least some heavily regulated industries are more likely than average to establish separate compliance committees, but even among these companies, specialized compliance committees are relatively uncommon. An analysis of the corporate governance documents for the top ten companies in the S&P 500 in the energy, finance, healthcare, and life sciences sectors found that only 15% of these companies delegate compliance oversight to a specialized committee, while the remaining 85% delegate compliance to the audit committee or another key committee. Large life sciences companies are the outlier, with 40% of the companies analyzed doing so. These findings are directionally consistent with the findings of others, who have similarly found that firms in heavily regulated sectors have above-average rates of compliance committee adoption, but even in these sectors, only a minority, and generally a small minority, have adopted such committees. Armour et al., for example, found that between 2004 and 2017, the heaviest adopters of compliance committees were companies in the banking (28%), healthcare (12.5%), pharmaceutical products (12.1%), medical equipment (8.6%), and industry business services (7.7%) sectors (Figure 5).[19]

Figure 5: Percentage of companies with specialized compliance committees



While audit committees may readily be able to oversee compliance in smaller companies or those in lightly regulated industries, such committees may not be equipped to handle complex regulatory compliance issues. In particular, audit committees may not have sufficient bandwidth to address regulatory compliance risk given competing demands. As a result, compliance issues may be given less time and attention than needed. Indeed, the Deloitte *Board Practices Report* found that almost 40% of the public company boards surveyed reported that their company's chief compliance officer did not regularly attend audit committee meetings, and 70% reported that the chief compliance officer did not regularly attend board meetings.[20] The same study found that 31% of boards reported discussing ethics and compliance topics only on an annual basis, and only 7% reported

discussing compliance and ethics at every board meeting.[21] Perhaps more importantly, audit committees often do not have members with special expertise or training in compliance issues. The *Board Practices Report,* for example, found that only 51% of boards surveyed reported that their board training includes content on ethics and compliance.[22]

Pros and cons of a separate compliance committee

This data raises the question of whether there is a disconnect between risk, particularly in heavily regulated industries, and the structural response of the boards of companies in those industries. So, should boards of companies in heavily regulated industries establish separate compliance committees?

Forming a separate compliance committee can be beneficial for a number of reasons, including, but not limited to, the fact that doing so:

- Elevates compliance as a corporate priority by establishing a clear "tone at the top";
- Allows boards to delegate compliance oversight to individuals with relevant expertise;
- Reduces the burden on the board as a whole and on other committees (e.g., audit committees) that may currently be handling compliance-related issues;
- Provides the chief compliance officer with a clear channel to discuss compliance concerns;
- Helps companies to adjust and adapt to rapidly evolving regulatory changes; and
- Sends a clear message to regulators and enforcement agencies that the company takes compliance seriously.

Most importantly, establishing a compliance committee may enhance the likelihood that a company avoids a significant compliance failure and, on a personal level, may reduce the risk that individual directors may be found liable for breaching their duty of care or loyalty.

There are also important potential challenges that should be fully considered before any major changes are made to board committees. For smaller companies, a separate compliance committee may not be necessary. For larger companies, adding another committee could create frustrations among board members, who often complain that there are too many committees and that they are already stretched too thin. Perhaps most importantly, separate compliance and audit committees could result in a disconnect between the committees, causing conflicting guidance or failure to identify and appropriately address overlapping or interrelated risks. Of note, NYSE companies that establish a separate compliance committee should ensure that the audit committee works with the compliance committee such that the audit committee continues to "assist board oversight" of "the listed company's compliance with legal and regulatory requirements," and that the audit committee continues to have responsibility for establishing whistleblower procedures relating to accounting and internal accounting controls and auditing matters; these responsibilities cannot be allocated to a different committee.[23]

Potential responsibilities of a compliance committee are, but are not limited to:

- Serving as eyes, ears, and voice of a full board on regulatory compliance issues;
- Serving as independent, regular point of contact for the chief compliance officer;
- Reviewing the annual risk assessment process;

- Reviewing the code of conduct, policies, procedures, and training;
- Reviewing compliance-related monitoring and audit reports;
- Reviewing hotline and other reports about compliance concerns;
- Reviewing root cause analyses;
- Assessing content and tone of regulatory interactions;
- Representing to board/company in key interactions with regulators, as necessary; and
- Overseeing regulatory crisis response.

Low-cost, high rewards

The risk of legal noncompliance—with attendant financial and nonfinancial penalties—is high in heavily regulated industries, and legal/regulatory compliance and compliance with product safety rules in such industries is often mission critical. Directors of companies in those industries have fiduciary obligations to implement and monitor corporate compliance systems, and failure to do so may result in unindemnifiable personal liability.

Notwithstanding this, many company boards have not established separate compliance committees to oversee compliance. Boards have wide latitude to determine how to best structure themselves, and compliance committees are not legally mandated. The Delaware Supreme Court, however, has acknowledged that failure to have a board committee overseeing mission-critical risks is a factor in determining whether directors have satisfied their fiduciary obligations. Boards of highly regulated companies should thus consider establishing specialized compliance committees with board members who have relevant specialized expertise. Doing so is a relatively low-cost initiative that has potential to produce high rewards.

Acknowledgments

The authors wish to acknowledge the generous contributions of Jennifer M. Haney and Rebecca Grapsas.

Takeaways

- Under rapidly evolving Delaware law, directors may face liability for failing either to implement or monitor corporate compliance.
- The risk of such liability is heightened for directors of companies that face mission-critical legal and regulatory risks and risks related to product safety.
- Such mission-critical risks are particularly common in heavily regulated industries, such as healthcare and life sciences.
- Courts will look to whether a board committee is engaged in mission-critical risks; the vast majority of companies do not currently have board committees specifically dedicated to overseeing legal and regulatory risks.
- Boards in heavily regulated industries should strongly consider establishing separate compliance committees to oversee legal and regulatory risk, and should assess whether the board is well-positioned to

oversee issues related to product safety.

1 Marchand v. Barnhill, 212 A.3d 805 (Del. 2019); In re Boeing Co. Derivative Litigation, 2019-0907 (Dec. Ch. Sept. 7, 2021); Teamsters Local 443 Health Servs. v. Chou, C.A. No. 2019-0816-SG (Del. Ch. Aug. 24, 2020); In re Clovis Oncology, Inc. Derivative Litigation, No. CV 2017-0222-JRS, 2019 WL 4850188 (Del. Ch. Oct. 1, 2019); Stone v. Ritter, 911 A.2d 362 (Del. 2006); In re Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996).
2 Stone, 911 A.2d at 370; In re Caremark, 698 A.2d at 969; In re Clovis Oncology, No. CV 2017-0222-JRS, 2019 WL 4850188, at *13.
3 Marchand, 212 A.3d at 809, 824; Teamsters Local 443 Health Servs., C.A. No. 2019-0816-SG at 52-53; In re Clovis Oncology, 2019 WL 4850188, at *13.
4 Teamsters Local 443 Health Servs., C.A. No. 2019-0816-SG at 53, 60, 67-68, 71; In re Clovis Oncology, No. CV 2017-0222-JRS, 2019 WL 4850188, at *12;
5 Marchand, 212 A.3d at 823.
6 Marchand , 212 A.3d at 821; Stone, 911 A.2d at 373.
7 Delaware General Corporation Law § 102(b)(7).
8 Marchand, 212 A.3d at 820-21.
9 In re: Boeing Co. Derivative Litigation, slip op at 33.
10 Department of Justice, *Fraud Statistics - Overview*, accessed September 9, 2021, https://bit.ly/3hkVtXk; Department of Justice, "Justice Department Recovers Over $4.7 Billion From False Claims Act Cases in Fiscal Year 2016," news release, December 14, 2016, https://bit.ly/3jXael3.
11 Department of Justice, "Justice Department Recovers Over $2.2 Billion from False Claims Act Cases in Fiscal Year 2020," news release, January 14, 2021, https://bit.ly/3tibgcX.
12 "Violation Tracker Summary for Primary Offense Type," Good Jobs First, accessed September 9, 2021, https://bit.ly/3A1kJcq.
13 Securities and Exchange Commission, Division of Enforcement, *2020 Annual Report*, accessed September 9, 2021, 17, https://bit.ly/3E1Qm8a.
14 Commodity Futures Trading Commission, Division of Enforcement, *FY2020 Division of Enforcement Annual Report*, accessed September 9, 2021, 8–9.
15 Sally Q. Yates, "Individual Accountability for Corporate Wrongdoing," memorandum, September 9, 2015, https://www.justice.gov/archives/dag/file/769036/download.
16 United States v. Park, 421 U.S. 658 (1975).
17 Spencer Stuart, *2020 U.S. Spencer Stuart Board Index*, accessed September 9, 2021, 22, https://bit.ly/3l6YRX3.
18 Deloitte, *Board Practices Report: Common threads across boardrooms*, March 2019, 14, https://bit.ly/3yXE7pD; John Armour, Brandon Garrett, Jeffrey Gordon, and Geeyoung Min, "Board Compliance," *Minnesota Law Review*, April 2019, 1,200, https://bit.ly/3BYELoA (data from 2004–2017 indicates that less than 5% of boards have separate compliance/risk committees).
19 Armour, Garrett, Gordon, and Min, "Board Compliance," 26 and 53.
20 Deloitte, *Board Practices Report*, 17.
21 Deloitte, *Board Practices Report*, 16; Robert Biskup, Krista Parsons, and Robert Lamm, "Board Oversight of Corporate Compliance: Is it Time for a Refresh?" *Harvard Law School Forum on Corporate Governance*, October 15, 2019, https://bit.ly/2YHdSY6.
22 Deloitte, *Board Practices Report*, 18.
23 See NYSE Listed Company Manual § 303A.07(b)(i)(A), (b)(iii); General Commentary to § 303A.07; Rule 10A-3(b)(3) of the Securities Exchange Act of 1934, as amended.