Conversations with the Board and Board Management

Alex Bahn

Cleo Belmonte

Stephanie Evans

Curtis Jewell

Alan Wilson

September 12, 2023

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

ACC Association of Corporate Counsel NATIONAL CAPITAL REGION

Capital One

ESAB

Agenda

- Structuring and Managing the Board Agenda and Meeting Materials
- Risk Oversight and Related Case Law Developments
- Trending Board Conversation Topics
  - Geopolitical and Economic Risks
  - Climate
  - Digital Assets and Artificial Intelligence
  - Cybersecurity
  - Anti-ESG
  - Human Capital
  - SEC Regulatory Developments
- M&A Opportunities and Integration Risks

Structuring and Managing the Board Agenda and Meeting Materials

Strategies for Managing Board Agenda and Materials

- Prepare a well-developed agenda
  - Consider outcomes of committee meetings and prior board meetings
  - Check against agenda for the same year-ago meeting
- Consider seeking input from the CEO and board chair at least two to three weeks before a board meeting

The content of board meeting agendas will vary, but all agendas should be reasonably detailed and include the following for each line item:

- Name of the item
- List of any supporting documents to be reviewed in connection with the item
- Presenter
- Basis for including the item (*e.g.*, is it informational, for board approval, etc.)
- Time allocation

Strategies for Managing Board Agenda and Materials

- Thorough board minutes are even more important today than in the past
  - In recent years, Delaware courts have narrowed corporations' defenses to stockholder books and records requests and, as a result, companies are often swamped with these demands
  - Properly documenting the board's deliberative process takes on heightened significance for "mission-critical matters" such as major deals or catastrophic events, where board actions may be the subject of stockholder litigation

There is no one-size-fits-all approach to drafting board minutes, and consistency in approach is important to maintain. Some common elements include:

- Date that the board meeting was noticed
- Who attended the meeting (including executives, employees and any outside advisers) and how they participated (in person or remotely)
- When the meeting commenced and adjourned
- If the board received presentations, whether to cite those or attach them as exhibits
- Issues considered, general inputs the board received, and reasonable details about the discussion

Sample Board Agenda

DATE

LOCATION

8-8:30	Breakfast Available
8:30	Meeting Called to Order
8:30-8:40	Approval of Minutes and Chairman Overview of Meeting
8:40-10:00	Committee Chair Reports
	[Names of committee chairs]
10:00-11:00	Management Update
	[Bulleted sub-topics with brief descriptions and designated speakers]
11:00 – 12:00	New Business
	[Bulleted description of topic(s) for board input and designated speakers]
12:00-12:15	Executive Session
12:15	Adjournment

Risk Oversight and Related Case Law Developments

Overview of Recent Developments

- Plaintiffs' lawyers frequently pursue claims based on alleged breaches of fiduciary duties, including the duty of oversight
- The frequency of oversight claims increased following a prominent June 2019 Delaware Supreme Court case involving a listeria outbreak at an ice cream company, where duty of oversight claims survived a motion to dismiss
  - Since then, at least seven claims against directors have survived a motion to dismiss
- In Jan. 2023, the Delaware Court of Chancery held for the first time that corporate officers also owe a duty of oversight and allowed a claim against an officer to proceed
  - This is likely to result in more frequent oversight claims against officers
  - At least two claims against officers have since survived a motion to dismiss

Evolution of the Duty of Oversight

Directors can rely on the honesty and integrity of management until they are confronted with red flags indicating the existence of wrongdoing

Absent cause for suspicion "there is no duty upon the directors to install and operate a corporate system of espionage to ferret out wrongdoing which they have no reason to suspect exists"

Allis-Chalmers (1963)

Caremark (1996)

When a claim of director liability for corporate loss is predicated upon ignorance of liability-creating activities within the company, only a sustained or systematic failure of the board to exercise oversight will establish the lack of good faith that is a necessary condition to liability

Stone v. Ritter (2006)

Establishes the current two-prong standard for holding directors or officers liable for oversight failures and the two resulting types of claims:

- **information-systems claims** (an outgrowth of Caremark)
- **red-flag claims** (an outgrowth of Allis-Chalmers)

Marchand v. Barnhill (2019)

Underscores that oversight function must be more rigorously exercised with respect to "mission critical" matters

The Caremark Standard for Oversight Liability

- The standard for holding directors or officers liable for oversight failures consists of two prongs and violating either can result in liability:
  - Utter failure to implement any reporting or information system or controls ("**prong-one**" or "**information-systems**" claims); or
  - Having implemented such a system or controls, conscious failure to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention ("**prong-two**" or "**red-flag**" claims)
- A breach of the duty of oversight is an act of bad faith in violation of the duty of loyalty
  - Unlike duty of care claims, duty of loyalty claims are non-exculpable
  - Plaintiffs must show bad faith, not just a weak and inadequate response or gross negligence
- Although Delaware courts have said claims for breach of the duty of oversight are "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win," motions to dismiss have been denied in at least seven cases since 2019

Understanding the Litigation Context for Oversight Claims

- Under Delaware law, the board of directors, not stockholders, manages the company's business and affairs, including the decision to initiate litigation
- A stockholder pursuing a claim on behalf of the company (*i.e.,* a derivative claim) must either make a demand on the board or show that demand would be futile
- To demonstrate demand futility, plaintiff must allege with particularity that a majority of the Board is interested or lacks independence; typically, a plaintiff argues that board members face a "substantial likelihood" of personal liability
  - At the motion to dismiss stage, the court is limited in what it can look at and must make all reasonable inferences in favor of the plaintiff
  - Plaintiffs are successfully using §220 "books and records" requests to obtain detailed information that they selectively include in their complaint to avoid dismissal
- A company that fails to have a case dismissed could ultimately prevail once it is able to fully present the facts, but the cost of litigation (and settlement) increases once a case survives a motion to dismiss

McDonald's Case Paves Way for Claims Against Officers

- In 2009, the Delaware Supreme Court expressly affirmed for the first time that "the fiduciary duties of officers are the same as those of directors"
- Taking that principle to its logical conclusion, in Jan. 2023, in a case involving sexual harassment allegations against the former Chief People Officer ("CPO") of McDonald's, a Delaware Court of Chancery for the first time expressly held that corporate officers also owe a duty of oversight
  - The court noted that officers may be in a better position to identify, address, and/or report red flags as compared to "part-time directors who meet a handful of times a year"
  - The court clarified that an officer's duty of oversight will typically be limited to the officer's areas of responsibility, but also noted that "particularly egregious red flag[s]" may trigger an officer's duty to act, even if it is outside the officer's domain
- In March 2023, the court dismissed similar Caremark claims against the directors of McDonald's, finding the directors had responded to red flags (while the CPO had not)

Key Takeaways for Directors

- Satisfying Caremark's oversight standard "envisions some degree of board-level monitoring system, not blind deference to and complete dependence on management"
- Board's oversight function must be "more rigorously exercised" with respect to compliance with laws, especially for "mission critical" regulatory matters and compliance, employee welfare and public safety risks
  - Such risks are often more apparent at companies with single-line business models
  - Chancery court's Oct. 2021 dismissal of claims involving Marriott suggests that cybersecurity has become a central compliance risk deserving of Board oversight at all companies
- Boards should create a record that reflects diligence in establishing appropriate systems, monitoring those systems, and following up on red flags
- The obligation to follow-up on red flags is not limited to mission critical matters

The standard for liability remains high:
plaintiffs must prove that the directors acted with scienter in a manner inconsistent with their fiduciary duties

Specific Actions for Boards to Consider

Caremark Standard	General
Prong One: **Utter failure to implement any reporting or information system or controls**	• Ensure management and the Board each has a process for identifying and regularly reviewing key risks (especially "mission critical" regulatory matters, legal compliance risks, employee welfare risks and public safety risks), and document those processes • Explicitly assign responsibility for oversight of key risks (either to the full Board or a committee) and include corresponding proxy disclosure; a separate risk committee is not required • Do not rely solely on the existence of regulatory requirements, including SEC or other reporting requirements, as a basis for assuming an adequate reporting system exists • Avoid being completely dependent on management reporting, by ensuring there are effective systems for employees and corporate partners to raise concerns and by regularly meeting directly with the chief compliance and risk officers • Establish an expectation and protocol for management to promptly report significant regulatory or compliance issues to the Board

Specific Actions for Boards to Consider

Caremark Standard	General
Prong Two: **Conscious failure to monitor or oversee operation of systems or controls**	• Remain vigilant for red flags and follow up when identified, including consideration of engaging outside advisors • Board/committee should receive regular reports on key risk and regulatory issues • Board minutes should demonstrate that the Board is regularly exercising oversight and following up on potential concerns while also being sensitive to preserving the confidentiality of any attorney-client privileged information • Exercise care in informal communications (*i.e.,* emails and texts) because such materials may need to be produced in response to a books and records request

Key Takeaways for Officers

- For matters within an officer's areas of responsibility, ensure reporting or information systems or controls are in place and well documented
- Be familiar with all the Company's key risks so you will be able to recognize and respond to red flags, including those that do not relate to your direct area of responsibility
- While there will likely be an increase in claims made against officers, unless a majority of the Board is interested, lacks independence or face a "substantial likelihood" of personal liability, the Board will retain general authority to determine whether a suit against an officer is in the Company's best interest
  - The claim against McDonald's Chief People Officer was ultimately dismissed based on a failure to plead demand futility
- The addition of an officer exculpation provision, as now permitted under Delaware law, does not eliminate the risk because oversight claims are non-exculpable loyalty claims
- Officers should understand the scope of their indemnification rights and available insurance

Trending Board Conversation Topics

Selected Geopolitical and Economic Risks

- US-China Tensions
- War in Ukraine
- Global Technology Decoupling
- Gulf Tensions
- Interest Rates
- Inflation
- Labor Participation Rates

Climate

- Climate disclosure frameworks continue to evolve
- SEC's proposed disclosure rules for climate disclosure remain outstanding, though are anticipated for the Fall
- Litigation is expected on any final SEC climate disclosure rules
- Many companies are taking steps to prepare for the new requirements, but practice is mixed

Climate – ISSB Standards

- On June 26, 2023, the International Sustainability Standards Board (ISSB) published its Climate-Related Disclosure Standard (the Climate Standard) as well as its General Standard For Sustainability-Related Financial Information (the General Standard).
- Although compliance with these standards is voluntary, the ISSB standards are expected to have a significant impact on the development of mandatory sustainability and climate disclosure regimes in the US and abroad.
- The ISSB standards provide a global baseline for sustainability disclosures, and include the following requirements for companies:
  - Disclosures related to management's role in assessing and managing climate-related risks and opportunities
  - Disclosures related to board mandates and composition as they relate to climate/sustainability risks and opportunities
  - Climate-related scenario analysis to assess the resilience of the entity's strategy (including its business model) to climate-related changes, developments or uncertainties
  - Disclosures related to its absolute Scope 1, 2 and 3 Greenhouse Gas (GHG) emissions

Cybersecurity

- Cyber-attacks are increasing in scope, scale and sophistication amid mounting geopolitical competition and rapid technological advancement.
- Critical government and private sector networks and infrastructure are vulnerable.
- Artificial intelligence (AI) could dramatically alter the threat landscape, increasing the risk of attacks and misinformation, while also providing defensive tools. Repeated attacks could cause significant economic and market disruption.
- The U.S. National Cybersecurity Strategy classifies ransomware as a national security threat and calls for more regulation and minimum standards for an expanded number of sectors.
- Recently adopted SEC cybersecurity disclosure rules expand company disclosure obligations and underscore need for strong cyber disclosure controls and procedures

Digital Assets / Artificial Intelligence (AI)

- Digital assets and AI continue to be a topic of interest for many companies
- Boards may want to first consider whether digital assets or AI present a business opportunity or threat to frame the company's strategic approach
- Boards should be aware of the degree to which AI is used by their company and management's systems for monitoring relevant AI legal developments (*e.g.*, state and federal regulatory regimes)
- Core areas to understand with respect to digital assets include:
  - Legal requirements, including securities or banking regulatory implications
  - Accounting treatment, including balance sheet and income statement presentation and effects
  - Implications for any existing financial or corporate treasury policies

Artificial Intelligence (AI) for Boards – Benefits and Risks

- As generative AI tools proliferate, directors should consider both (1) the degree to which information they receive from management, auditors, consultants, or others may have been produced using generative AI and (2) whether they can and should use generative AI tools as an opportunity to support their duties and activities as directors.
- For both purposes, directors should be mindful of risks associated with the company's use and reliance on generative AI. Some key considerations include:
  - **Duties**: Generative AI are machines, not people. Unlike directors, generative AI owes no fiduciary duties and faces no liability for breach.
  - **Accuracy**: Generative AI can be a valuable tool, but generative AI results may be inaccurate, incomplete, or biased. Accordingly, outputs must be scrutinized and tested for trustworthiness.
  - **Confidentiality**: Generative AI retains user interactions as training data. This improves the quality of its output in future versions, but also implicates privacy and cybersecurity risks, including the unintended disclosure of confidential information.

Chatbots and Generative AI – Top 10 Business and Legal Risks

1. **Contract** – confidentiality limitations and other control requirements may apply
2. **Cybersecurity** – chatbots can create malware and be used for social engineering, phishing and malicious advertising schemes
3. **Data privacy** – user-consent options and opt-out controls may not comply with evolving laws
4. **Deceptive trade practices** – outsourcing work to a chatbot or AI software when a consumer believes they are dealing with a human can be an unfair and deceptive practice
5. **Discrimination** – bias can result from AI systems, purposefully or by virtue of the datasets used to train AI
6. **Disinformation** – malicious actors can use chatbots to create false, authoritative-sounding information at mass scale quickly
7. **Ethical** – professional obligations may restrict use of AI
8. **Government contracts** – use of AI in preparing bids could result in similar bids and appear as though competitive information was shared with competitors, which is prohibited; AI restrictions might also be included in government contract awards
9. **IP** – outputs may infringe on IP rights, and ownership over AI outputs may be in dispute
10. **Validation** – chatbots are known to produce errors, making validation controls essential

Anti-ESG

- Companies increasingly cannot avoid taking positions on big social issues of the day
  - *E.g.*, Abortion, LGBTQ+, DEI
- Several, mostly Republican-led, states have adopted or introduced legislation aimed at limiting use of ESG factors in financial decision-making for state funds and constraining discretion of banks in making loans
- Anti-ESG shareholder proposals more than doubled in the past three years, though support for those making it to a vote remains low
- Boards should stay aware of these developments, keeping in mind the company's strategy and mission, and consider discussing with management how the company might plan to respond to a new, big issue

Human Capital

- Navigating the future of remote/hybrid work continues to dominate the challenges facing companies
- Boards (or committees tasked with HCM oversight) may want to consider the following:
  - How is the company approaching HCM in designing its overall hiring and succession planning strategy?
  - Does the company have appropriate role descriptions that align with its HCM strategy?
  - Has the company's long-term remote work policy been aligned with the company's IT leaders?
  - How is the board and company responding to stakeholder expectations for HCM?
  - Does the C-suite have sufficient resources to manage HCM?

SEC Regulatory Developments

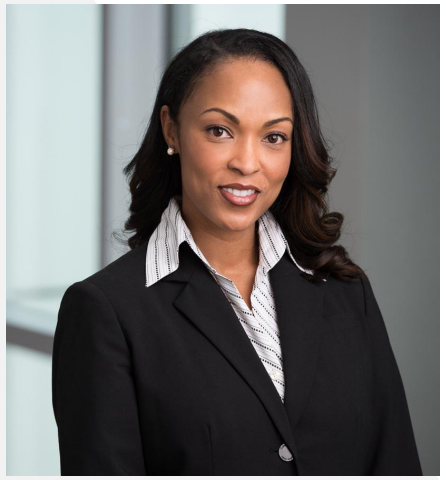
- SEC has been taking an aggressive approach to public companies, combined with senior staff turnover
- Relentless rulemaking agenda with short comment and implementation periods
- New rules demonstrate that the SEC is unwilling to seek middle ground and make an effort to reduce complexity
- Recent SEC enforcement cases rely heavily on the requirements for disclosure controls and procedures (*e.g.*, non-GAAP, ESG and cyber)
- Cybersecurity disclosure rules will require boards and management to give fresh consideration to their oversight and governance around cybersecurity and to ensure that controls and procedures are appropriately designed to satisfy new disclosure requirements about material cyber incidents

M&A Opportunities and Integration Risks

M&A Opportunities and Integration Risks

- Economic, geopolitical and regulatory pressures generally seem to be sidelining M&A activity
- Boards of well-capitalized companies, though, are increasingly focusing on M&A activity to gain an advantage over less-capitalized competitors and to overcome challenges from pursuing organic growth alone
- Boards should be mindful of continued and increasing antitrust scrutiny and cross-border obstacles when evaluating M&A opportunities, *e.g.*:
  - **FTC** – despite some public losses (*e.g.*, Microsoft/Activision), the FTC remains committed to harsh scrutiny, particularly of potential competitive harm from vertical and conglomerate mergers, entrenchment of firms with dominant positions, potential competition, acquisitions of minority interests, labor markets, and transactions involving platforms
  - **Reverse CFIUS** – recent Biden Executive Order would prohibit and require notification of certain outbound investments into China, Hong Kong and Macau in respect of semiconductor / microelectronics, quantum information technologies and AI industries

Speaker Biographies



Cleo Belmonte
cleo.belmonte@capitalone.com

Cleo Belmonte leads the Governance and Securities function within the Capital One Legal Department where she provides legal and strategic advice to the company's board of directors and senior executives, including the company's Chief Executive Officer and Chief Financial Officer regarding all aspects of corporate governance, public disclosure, investor relations, executive compensation, environmental, social and governance matters, as well as compliance with federal and state corporate and securities laws and NYSE regulations.

Ms. Belmonte joined Capital One in 2015 and has served in roles of increasing responsibility since that time. Prior to Capital One, Ms. Belmonte was the Vice President, Associate General Counsel and Assistant Secretary of EchoStar Corporation and Hughes Communications, Inc. where she led Corporate Law Group of the company's legal department and was responsible for the oversight of securities corporate governance, mergers and acquisitions, employment, and data privacy and security for the companies and their more than 100 domestic and international subsidiaries.

Prior to EchoStar and Hughes, Ms. Belmonte was an associate in the law firms of Squire Patton Boggs LLP and Pillsbury Winthrop LLP.

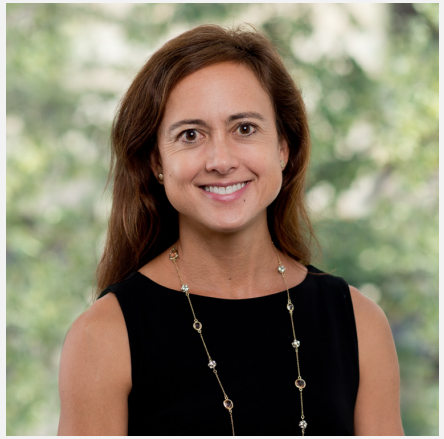
Curtis Jewell
Curtis.Jewell@esab.com

Curtis Jewell serves as ESAB Corporation's General Counsel and Corporate Secretary. He leads the Corporation's legal team, advises the executive team on legal strategy, and acts as the Corporation's legal representative. Jewell became ESAB Corporation's general counsel in 2020 and was appointed Senior Vice President and Corporate Secretary in 2022. He has significant experience leading legal teams through complex acquisitions and cross-border initiatives while driving process improvement.

Prior to his appointment at ESAB Corporation, Jewell was the Corporate Secretary of Colfax Corporation, where he held roles of increasing responsibility since joining in February 2011. Before joining Colfax, Jewell was in private practice at Hogan Lovells LLP, where he focused on securities law, corporate governance, mergers and acquisitions, and capital market transactions. He began his legal career at Schulte Roth & Zabel in New York City.

Alex Bahn
Alex.Bahn@wilmerhale.com

Alex Bahn advises clients on a broad range of corporate governance, securities compliance and disclosure, and capital markets related matters. Mr. Bahn regularly advises on understanding and addressing SEC reporting and disclosure requirements, stock exchange listing requirements, beneficial ownership and short-swing liability avoidance, insider trading considerations, securities registration exemptions, as well as financing transactions, including capital markets offerings and commercial paper programs. Mr. Bahn frequently helps NYSE and Nasdaq-listed companies and their boards navigate annual meeting and proxy-related issues, including shareholder proposals, executive compensation disclosure requirements, investor communications and proxy advisory firm recommendations. Clients routinely turn to him for assistance with particularly sensitive disclosure and governance matters, such as leadership transitions and related party transactions.



Stephanie Evans
Stephanie.Evans@wilmerhale.com

Stephanie Evans advises domestic and international clients on a wide range of corporate transactions, with a particular focus on mergers and acquisitions, joint ventures, strategic alliances and financings. She regularly advises boards and special committees in connection with transactions and provides advice on governance and commercial transactions. Her clients include private and public companies in a variety of industries, including financial services, defense and technology. She is active with emerging growth companies throughout their development cycle (see more on Ms. Evans' emerging growth company practice on WilmerHaleLaunch.com). She was previously Vice Chair of the Corporate Practice Group. Ms. Evans also worked as an associate in the Global Investment Banking Group of Deutsche Banc.

Alan Wilson
Alan.Wilson@wilmerhale.com

Alan Wilson routinely advises public and private company clients on a variety of matters concerning corporate governance and compliance with federal securities laws, particularly with regards to the intersection between law and accounting. This includes advice on SEC disclosures, ESG matters, stakeholder engagement, shareholder proposals, formal and informal investor communications, capital markets transactions, mergers and acquisitions, and joint ventures. Additionally, he routinely assists companies, boards and board committees in navigating internal investigations, enforcement inquiries, and whistleblower allegations. Mr. Wilson is also Chair of the ABA Business Law Section Law and Accounting Committee, a Massachusetts CPA, and a member of the National Conference of Lawyers and CPAs, Massachusetts Society of CPAs, and the American Academy of Attorney-CPAs.

APPENDIX – SELECTED DUTY OF OVERSIGHT CASE LAW SUMMARIES

In re The Boeing Co. Derivative Litigation (DE Ch. Ct.; 9/7/21)

Aerospace manufacturer's new 737 MAX passenger airplane suffered two fatal crashes (one in October 2018 and the second in March 2019) that took 346 lives and lead to an extended grounding of the 737 MAX.

Prong One: Utter failure to implement any reporting or information system or controls	Prong Two: Conscious failure to monitor or oversee operation of system or controls
Court allowed case to proceed on following allegations: • Board had no committee charged with direct responsibility to monitor airplane safety • Board did not monitor, discuss or address airplane safety on a regular basis • Lack of an internal reporting system by which whistleblowers and employees could bring safety concerns to the Board's attention • Absence of process or protocol requiring management to apprise the Board of airplane safety issues	*Court also indicated that plaintiffs adequately pleaded a Prong Two claim based on the following allegations:* • Board's passive acceptance of CEO's safety assurances following the first 737 MAX crash and after media reports of safety issues

Status: In Nov. 2021, the current and former Boeing directors reached a $237.5m agreement (funded by insurance) to settle these claims. Boeing also agreed to hire an ombudsman to handle internal issues and appoint a board member with experience in aviation safety. There was no admission of wrongdoing.

Fireman's Retirement System of St. Louis v. Sorenson, et al (Marriott) (DE Ch. Ct.; 10/5/21)

In 2018 Marriott discovered a data security breach, perpetrated since 2014 through the reservation database of a hotel chain it acquired in 2016, that exposed personal information about 500 million guests. Marriott first received an alert of a potential issue on Sept. 7, 2018. The Board was informed on Sept. 18, 2018 and Marriott's first public disclosure was on Nov. 30, 2018.

Prong One: Utter failure to implement any reporting or information system or controls	Prong Two: Conscious failure to monitor or oversee operation of system or controls
In dismissing the prong one claim, the court said that: • Demand was not excused because none of the director defendants faced a substantial likelihood of liability on a non-exculpated claim • Marriott's Board consistently ranked cybersecurity as one of the Company's primary risks • The Board and its audit committee were routinely apprised of cybersecurity risks and mitigation and received annual reports on the Company's Enterprise Risk Assessment that specifically evaluated cyber risks • The Company engaged outside consultants to improve, and auditors to audit, corporate cybersecurity practices • Marriott had internal controls over its public disclosure practices • Management provided the Board with the information and reports plaintiff described as red flags	*In dismissing the prong two claim, the court said that:* • Plaintiffs had not "pleaded with particularity that the Post-Acquisition Board learned of legal or regulatory violations. And even if it had, the Board did not consciously choose to remain idle" • Pleading non-compliance with non-binding industry standards (*e.g.*, PCI DSS) is not the same as pleading directors knowingly permitted violation of positive law • Simply listing statues "in vague, broad terms" without alleging what law was violated and how is insufficient • There were no properly pleaded allegations of "known illegal conduct, lawbreaking, or violations of a regulatory mandate" • There were no properly pleaded allegations that the Board knew personal data was accessed such that state law notification obligations had been triggered prior to Nov. 2018

Status: Court dismissed claims

City of Detroit Police & Fire Ret. Sys. v. Hamrock (NiSource) (DE Ch. Ct.; 6/30/22)

In 2018 in Lawrence, Mass., construction crew of energy company NiSource improperly replaced a cast-iron pipe causing a flow of high-pressure gas resulting in explosions that killed one, injured 22 and damaged 131 structures. Echoing *Marchand*, plaintiffs alleged that defendants failed to implement a monitoring system to oversee "mission-critical" pipeline safety.

Prong One: Utter failure to implement any reporting or information system or controls	Prong Two: Conscious failure to monitor or oversee operation of system or controls
In dismissing the prong one claim, the court said that: • While pipeline safety was "mission-critical" to NiSource, records showed that Board's Environmental, Safety and Sustainability ("ES&S") Committee closely monitored safety risks • The ES&S Committee held five formal meetings in the three years leading up to the explosion, regularly received extensive reports from senior executives, and regularly reported directly to the Board • The ES&S Committee regularly monitored internal safety policies, company-wide and industry-wide gas safety incidents, and federal, state and local rules and regulations	*In dismissing the prong two claim, the court said that:* • Despite knowledge that poor recordkeeping practices posed risks and violated federal pipeline safety regulations at other subsidiaries, these risks were too general and attenuated from the root causes of the explosions • It is unreasonable that a generalized failure to comply with an expansive regulation at one subsidiary could have alerted the Board to the specific risk at another subsidiary • The fact that the Board and ES&S Committee were aware of these general risks indicates that the reporting system was working as it should

Status: Court dismissed claims

Giuliano v. Fleming (In re Nobilis Health Corp.) (US Bankr. Ct. Dist. DE; 7/27/22)

Nobilis, an owner of surgical facilities and clinics, in mid-2017 began overvaluing certain long-term accounts receivables pledged as collateral for loans. Noblis eventually had to write down $72 million of receivables and filed for bankruptcy protection in October 2019. The Chapter 7 Trustee for Nobilis initiated an adversary proceeding against the former directors and officers of Nobilis.

Prong One: Utter failure to implement any reporting or information system or controls	Prong Two: Conscious failure to monitor or oversee operation of system or controls
Not addressed by court	*With respect to the prong two claim, the court said that:* • Directors and officers continued to carry older receivables on the Company's books, which gave a false picture of its financial health • Directors and officers concealed changes in accounting policies from Company auditors, even convincing an "unsuspecting auditor to sign off on the Company's 10-K for fiscal year 2017" • CFO was informed by a physician that the physician's attorney considered aspects of the company's "split billing" practices to be illegal, *i.e.*, creation of separate claims that would be submitted to insurers for incidental procedures

Status: Discovery ongoing as of July 2023

Constr. Indus. Laborers Pension Fund v. Bingle (Solarwinds) (DE Ch. Ct.; 9/6/22)

In December 2020, Solarwinds, an IT software company, discovered a data security breach, perpetrated by hackers since January 2019 through the company's software, which allowed hackers to access and steal proprietary information, confidential emails, and intellectual property from up to 18,000 clients. Company disclosure of the breach caused its stock price to drop 40%.

Prong One: Utter failure to implement any reporting or information system or controls	Prong Two: Conscious failure to monitor or oversee operation of system or controls
In dismissing the prong one claim, the court said that: • The Nominating and Corporate Governance Committee met and discussed cybersecurity risks before and after a management presentation, prompting an April 2019 amendment to the Company's charter to address cybersecurity issues • Even though the NCG Committee never reported to the full Board on the subject in the 26 months since Company's IPO, the mere passage of time didn't implicate bad faith due to the lack of the NCG Committees' "awareness of a particular threat, or understanding of actions the Board should take"	*In dismissing the prong two claim, the court said that:* • Board was not made aware of departing Global Cybersecurity Strategist's resignation email in which he complained to the Chief Marketing Officer that his requested changes weren't implemented • Board was not made aware of weak, "elementary-level" password "solarwinds123" in place in a manner that could've compromised Company security from early 2017-November 2019; the issue was only fixed when a third-party informed Company of security deficiency • Presentation by Company executives to NCG Committee on company-specific cybersecurity risks "was not indicative of an imminent corporate trauma"

Status: Court dismissed claims

In re McDonald's #1 [Officer] (DE Ch. Ct.; 1/26/23)

A corporate culture described as a "party atmosphere," in which the Chief People Officer ("CPO") and CEO of McDonald's reportedly committed acts of sexual harassment from 2015-2019, caused the Company to suffer harm in the form of employee lawsuits, lost employee trust, and a damaged reputation. This decision covers claims against the CPO in his capacity as officer.

Prong One: Utter failure to implement any reporting or information system or controls	Prong Two: Conscious failure to monitor or oversee operation of system or controls
Not addressed by court	*Court indicated that plaintiffs adequately pleaded a Prong Two claim and allowed case to proceed on following allegations:* • Litany of HR complaints, EEOC complaints, employee strikes associated with EEOC complaints in ten cities, and letters from U.S. Senators from 2015 up and until the CPO's termination with cause in 2019 • 2016: CPO engaged in acts of sexual harassment shortly after EEOC complaints and employee strikes highlighting the Company's sexual harassment issues • 2019: CPO again engaged in acts of sexual harassment after working with management on ways to address the Company's sexual harassment issues

Status: Case subsequently dismissed for failure to plead demand futility following dismissal of claims against directors in McDonald's #2 on March 1, 2023

In re McDonald's #2 [Directors] (DE Ch. Ct.; 3/1/23)

A corporate culture described as a "party atmosphere," in which the Chief People Officer ("CPO") and CEO of McDonald's reportedly committed acts of sexual harassment from 2015-2019, caused the Company to suffer harm in the form of employee lawsuits, lost employee trust, and a damaged reputation. This decision covers claims against the directors.

Prong One: Utter failure to implement any reporting or information system or controls	Prong Two: Conscious failure to monitor or oversee operation of system or controls
Not addressed by court	*In dismissing the prong two claim, the court said that:* • The Board only indisputably became aware of the CPO's misconduct in November 2018, when thirty employees witnessed him physically pull an employee onto his lap • Upon becoming aware of the issue in November 2018, the Board immediately responded to the sexual harassment issue and received reports on the issue from management • In June 2019, management presented a memo to the Strategy Committee outlining steps the Company was taking to address the sexual harassment issue, including retaining sexual harassment professionals to design new policies • Upon learning of subsequent inappropriate behavior, the Board terminated the CEO without cause and the CPO with cause

Status: Court dismissed claims against directors

Ont. Prov. Council of Carpenters' v. Walton [Walmart] (DE Ch. Ct.; 4/26/23)

Walmart, both a dispenser and wholesale distributor of prescription opioids, entered into a confidential settlement with the DEA in 2011 obligating it to implement and maintain a compliance program for all of its pharmacies. Plaintiffs allege that management decisions prioritizing profits over compliance, overseen by board and board committees, caused Walmart to breach the DEA settlement and violate the Controlled Substances Act. The fallout of the alleged breaches contributed to the proliferation of opioids, prompting lawsuits settled by Walmart for $3.1B in 2022.

Unlike the other cases, Vice Chancellor Laster's opinion analyzed Prong One, Prong Two, and *Massey* claims (whether defendants knowingly caused the Company to seek profit by violating the law) together, focusing on whether defendants' conduct constituted bad faith.

While plaintiffs' claims against defendants for Walmart's role as a distributor of opioids were dismissed, plaintiffs adequately alleged particularized facts supporting an inference of bad faith by defendant officers and directors for Walmart's role as dispenser under the Controlled Substances Act:

- Aggressive document redactions for non-responsiveness and privilege in defendants' Section 220 production led to an inference of inaction or that "[a]ll they did was receive and consider legal advice"
- Management, the Board and/or the Audit Committee were informed on specifics that confirmed non-compliance with the 2011 DEA Settlement, including (i) where project statuses were color-coded as green for "on schedule," yellow for "watch list," and red for "major issues," the controlled substance compliance program was labeled red; (ii) internal emails asserting that the compliance program was underfunded by $30M; (iii) photos of patrons at 7 a.m. waiting in-line at a pharmacy with a "very high number of prescriptions for Oxycodone"; and (iv) a pharmacist whistleblower suit leading to the pharmacist's termination
- Citing *McDonald's I*, the Court reiterated that officers had oversight duties

Status: SLC motion to stay granted – stay remains in effect as of July 2023