Wachtell, Lipton, Rosen & Katz

Risk Management and the Board of Directors

March 2024

Risk Management and the Board of Directors

I. INTRODUCTION

Overview

Public companies and their boards of directors face an increasingly complex array of risks that test the resilience of corporate values, strategies, operations, and enterprise risk management frameworks. Tighter monetary policies, deepening geopolitical tensions, widening domestic political polarization, labor shortages, severe weather events, growing challenges tied to nature and biodiversity loss, and the uncertainties surrounding generative AI are among the varied risks that companies have had to contend with in recent years.

These risks are likely to persist and even intensify—against the backdrop of an election year in the United States, ongoing conflict in Ukraine and the Middle East, and China's sluggish post-pandemic recovery. Severe wildfires, heatwaves and flooding across the globe, rising insurance costs, and the exodus of insurers from large pockets of the country underscore the burgeoning financial risks and challenges of climate risks. Cybersecurity risk continues to increase in scale and scope while the geopolitical rivalry between China and the United States remains unabated. According to the World Economic Forum's Global Risks Report 2024, the majority of the business leaders polled anticipate some instability and a moderate risk of global catastrophes, while another 30% expect even more turbulent conditions over the next two years.

All of this underscores the corporate imperative to continually reassess risk profile and exposure, and to adapt policies and processes accordingly. Managing corporate risk is not just the business and operational responsibility of a company's management team—it is a governance and strategic issue that is squarely within the oversight responsibility of the board. Courts and regulators are increasingly scrutinizing board-level risk oversight mechanisms, as well as the adequacy of public disclosures and the quality of board responses when crises erupt. Recent *Caremark* decisions from the Delaware Court of Chancery continue to set a very high bar for claims of oversight failure, but have also allowed some claims to proceed beyond the motion to dismiss stage where the allegations show a bad-faith failure to appreciate and oversee core risks to the company's business. Pressure from institutional and activist investors, state law-enforcement authorities, and federal administrative agencies also continues to mount.

This guide identifies critical risk-management issues that merit close attention by directors and management, and surveys the sources of risk oversight obligations borne by boards of directors, including Delaware law developments highlighting the importance of active, engaged board risk oversight (and maintaining appropriate records of that oversight), as well as U.S. Securities and Exchange Commission (SEC) and New York Stock Exchange (NYSE) rules, input from investors and proxy advisory firms, and U.S. Department of Justice (DOJ) expectations. We end with a set of recommendations for improving risk oversight overall, including specific advice for managing sustainability, cybersecurity, data privacy, and other environmental, social, and governance (ESG) risks.

Risk Oversight by the Board—Not Risk Management

Both the law and common sense continue to support the proposition that boards cannot and should not be involved in day-to-day risk *management*. However, every board's *oversight* role should include active engagement in monitoring key corporate risk factors, including through appropriate use of board committees. These board-level monitoring efforts should be documented through minutes and other corporate records.

Directors should—through their risk oversight role—require that the CEO and senior executives prioritize risk management and integrate risk management into strategic decision-making. Directors should satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's strategy and business purpose, and that these policies and procedures are functioning as intended. The board should be familiar with the type and magnitude of the company's principal risks, as well as new and emerging risks, especially concerning "mission critical" areas for the business and the sector, and should be kept apprised periodically of the company's approach to identifying and mitigating such risks, instances of material risk management failures, and action plans for mitigation and response. Directors may also need to consider the appropriate allocation of oversight responsibilities among the board and its committees, including whether dedicated ad hoc or standing committees may be necessary to focus oversight on particular risk areas. In prioritizing such matters, the board can send a message to management and employees that comprehensive risk management is an integral component of strategy, culture, and business operations.

The board's risk oversight role has been brought into sharp focus with the recent publication of the Boeing Report, an assessment of the effectiveness of risk management systems with respect to safety at The Boeing Company prepared by a panel of aviation experts, the release by the Federal Aviation Administration of the results of its audit of Boeing and Spirit AeroSystems, which found multiple instances of non-compliance in Boeing's manufacturing process control, parts handling and storage, and product control, and Boeing's testimony before a Senate Commerce Committee regarding the company's cooperation in a governmental probe into recent safety incidents. The situation at Boeing serves as an important reminder that the board's role is not only to establish risk management systems appropriately tailored to the material risks the company faces, but also to oversee the operation of these systems to ensure that they are embedded company-wide and are, in practice, followed throughout the organization. See our recent memo, The Boeing Report: A Reminder of the Board's Indispensable Role in Risk Oversight.

Tone at the Top and Corporate Culture as Key to Effective Risk Management

The board and relevant committees should work with management to set the appropriate "tone at the top" by promoting and actively cultivating a corporate culture that meets the board's expectations and aligns with the company's strategy. Directors not only can help steer the company through a complex economic environment, but can serve as a sounding board for the company's public positions on social and political issues of importance to the company's various stakeholders—employees, customers, suppliers, and stockholders alike. In setting the appropriate tone at the top, transparency, consistency, and communication are key.

The board's vision for the corporation should include its commitment to risk oversight, ethics, good corporate citizenship, and avoiding compliance failures, and this commitment should be communicated effectively throughout the organization. The board's response to new challenges should be deliberate but prompt; undue delay can harm a company's relationships with stakeholders and tarnish the company's reputation and brand image. This is particularly important when the challenges involve employee safety and well-being, and in industries where product or service failures can jeopardize consumer or environmental safety or critical infrastructure. Corporate culture should not prioritize cost-cutting or profits (which may include, as a matter of employee and public perception, compensation levels) over safety and compliance.

Growing scrutiny over diversity, equity, and inclusion (DEI) initiatives and practices has added pressure on boards to set the appropriate tone at the top. Discrimination and harassment can have a devastating impact not just on directly affected employees, but also on broader corporate culture, employee morale and retention, consumer preferences, and the reputation of the company, its board and management. Delayed or indecisive responses to misconduct can often be as damaging to a company as the misconduct itself. Ensuring an inclusive workplace environment is central to employee morale and a motivated workforce.

With respect to these and other critical risks, the board should work with management to consider developing a crisis response plan that includes the input of human resources and talent management personnel, legal counsel, and other external advisors in addition to senior management with direct oversight over risk reporting and management. The use, scope, and design of preventative corporate policies, including training and educational programming related to conduct and reporting expectations, should also be carefully considered, as should potential implications, enforcement, and remedies in the event of a violation once such policies are adopted. Disclosure of board-level participation in these deliberations also may be key to demonstrating to internal and external audiences the seriousness of these policies.

Promoting Board Readiness for Current and Future Risk Oversight

To prepare effectively for today's dynamic risk environment, boards should continue to engage in regular director training to build on existing skills and leverage management and advisor expertise to develop knowledge and experience concerning issues that may affect their companies. Plans for recruiting new directors should take into consideration any potential knowledge, skill, and background gaps. That does not mean every board must have subject matter expertise in all key risk areas, but thought should be given to enhancing the experience and learning of—and the outside advisor support for—the board's membership as the company's risk profile and the business environment evolve. As stakeholder expectations continue to mount, some boards may also consider preparing to assume a more public-facing role on key issues, including by engaging with stakeholders beyond the traditional corporate engagement cycle.

II. SOURCES OF RISK OVERSIGHT OBLIGATIONS OF THE BOARD OF DIRECTORS

Although institutional investors, legislators and other constituencies have varying expectations concerning board risk oversight responsibilities, the core responsibilities are grounded principally in state law fiduciary duties, federal and state laws and regulations, stock exchange listing requirements, and certain established (albeit evolving) best practices frameworks.

Recent Delaware decisions highlight the importance of creating and maintaining a clear record of appropriate risk oversight. They also show the importance of making a good faith effort to put in place a compliance system designed to help the board reasonably ensure that the company operates within the bounds of the law and that its products, services, and operations do not cause harm to consumers, community members, or the environment.

Fiduciary Duties

The Delaware courts have taken the lead in formulating legal standards for directors' risk oversight duties, particularly following *In re Caremark International Inc. Derivative Litigation*, the seminal 1996 decision defining the scope of director liability for the corporation's failure to comply with external legal requirements. The *Caremark* line of cases has held that directors can be liable under breach of fiduciary duty for a failure of board oversight only where there is "sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists" or a deliberate failure to monitor an existing system resulting in a disregard of a pattern of "red flags." Delaware Court of Chancery decisions in the decades following *Caremark* regularly dismissed shareholder suits claiming such a total failure of oversight responsibility. *See*, for example, our memos discussing *In re The Goldman Sachs Group, Inc. Shareholder Litigation* (2011), *Oklahoma Firefighters Pension & Retirement System* v. *Corbat* (2017), and *City of Birmingham Retirement and Relief System* v. *Good* (2017).

More recent rulings, however, show that the risk of exposure for failure of oversight is real, and that courts are willing to permit stockholder claims alleging breaches of fiduciary duty by directors to proceed to discovery where the complaint alleges with specificity that the board ignored red flags reflecting underlying compliance, safety, reporting or other risks or that the board gave insufficient attention to such matters, despite the existence of company-wide policies and procedures on the topic. These decisions have denied motions to dismiss claims that boards failed to act in good faith to maintain board-level systems for monitoring mission critical functions, such as product safety, pharmaceutical trial testing, and financial reporting. A history of unaddressed deficiencies and a failure by the company to provide books and records documenting active board supervision of the compliance and risk assessment functions have been among the chief aggravating factors driving these judicial decisions. *See, e.g.*, *Hughes* v. *Hu*; *Marchand* v. *Barnhill* (Bluebell Creameries); *In Re Clovis Oncology Inc. Derivative Litigation*; *In Re The Boeing Company Derivative Litigation*; *Lebanon County Emps. Ret. Sys.* v. *Collis*; *Ontario Provincial Council of Carpenters' Pension Trust Fund* v. *Walton*.[1]

That said, *Caremark* claims do not eviscerate the protections of the business judgment rule, as we have written. Delaware courts continue to recognize that only "a deliberate failure to act" will give rise to failure-of-oversight liability and that board risk management and compliance structures can go a long way in protecting directors against fiduciary breach claims. *See, e.g.*,

[1] Delaware courts in the *Caremark* line of cases have pointed to the absence of such documentation produced in response to a stockholder's inspection demand as a basis to infer that the directors "fail[ed] to act in good faith to maintain a board-level system for monitoring the Company's financial reporting." *Hughes* v. *Hu*, 2020 WL 1987029, at *17 (Del. Ch. Apr. 27, 2020).

Firemen's Retirement System of St. Louis v. *Sorenson*; *City of Detroit Police and Retirement Sys. v. Hamrock*; *Clem v. Skinner*. Having documented control and monitoring functions commensurate with the scope and scale of a company's risks is therefore critical.

SEC Risk Disclosure Rules

The SEC requires companies to disclose the board's role in risk oversight, the relevance of the board's leadership structure to such matters, and the extent to which risks arising from a company's employee compensation policies are reasonably likely to have a "material adverse effect" on the company. A company must further discuss how its compensation policies and practices, including those of its non-executive officers, relate to risk management and risk-taking incentives. And the SEC requires companies to disclose in their annual reports "factors that make an investment in [a registrant's securities] speculative or risky." Recent SEC comment letters issued to companies have asked for enhanced proxy statement disclosures by companies that would provide additional company-specific detail on the board's role in risk oversight and the relationship between the board's leadership structure and risk management matters. The SEC has also issued sample comment letters addressing specific timely issues. Following the start of the war in Ukraine, for example, the SEC released a sample comment letter seeking disclosures on companies' risks in the region. The SEC issued a similar comment letter concerning China.

Recently announced SEC rules expand disclosure requirements concerning climate, and upcoming rulemakings are expected to similarly expand disclosure obligations related to human capital management and board diversity matters. In 2023, the SEC also adopted sweeping cybersecurity risk disclosure rules, which are discussed further in Section VII of this memo.

In late 2022, the SEC finalized the adoption of amendments to the rules governing Rule 10b5-1 trading plans. Among other things, the amendments require a mandatory "cooling-off" period after a plan is adopted or amended and before trading can begin, increased disclosure regarding an issuer's insider trading policies and procedures (or an explanation of the absence of such policies) in its annual proxy statement or Form 10-K, and a condition that all persons entering a Rule 10b5-1 plan act in good faith with respect to the plan. These amendments, together with changes to share repurchase disclosures adopted last year, underscore the need for companies to remain vigilant about securities trading policies and compliance processes. The SEC has demonstrated its eagerness to bring aggressive enforcement actions in this area, with a settled case in November 2023 against Charter Communications. The SEC obtained a $25 million penalty against Charter based on technical deficiencies in a 10b5-1 plan, in the absence of any allegation that the company possessed material nonpublic information when it carried out repurchases pursuant to the defective plan.

Stock Exchange Rules

NYSE corporate governance standards impose certain risk oversight obligations on the audit committee of a listed company. Specifically, while acknowledging that "it is the job of the CEO and senior management to assess and manage the listed company's exposure to risk," the NYSE requires that an audit committee "discuss guidelines and policies to govern the process by which risk assessment and management is undertaken." These discussions should address major financial risk exposures and the steps management has taken to monitor and control such

exposures, including a general review of the company's risk management programs. The NYSE permits a company to create a separate committee or subcommittee to be charged with the primary risk oversight function as long as the risk oversight processes conducted by that separate committee or subcommittee are reviewed in a general manner by the audit committee and the audit committee continues to discuss policies with respect to risk assessment and management.

In 2022, the SEC adopted a final rule requiring stock exchanges to update their applicable listing standards to require companies to maintain a compensation clawback policy, introducing a new compliance obligation to be overseen by the board. Under the final rules, an issuer must adopt a policy that requires it to recover from executive officers incentive compensation that would not have been earned based on specified accounting restatements. Importantly, the new rules limit board discretion with respect to clawbacks: an issuer is required to recover compensation in compliance with its recovery policy, except to the extent that pursuit of recovery would be impracticable because it would: (1) impose undue costs on the issuer, (2) violate home country law based on an opinion of counsel, or (3) cause a broad-based retirement plan to fail to meet the tax-qualification requirements. Before concluding that pursuit is not feasible, the issuer must first make a reasonable attempt to recover the incentive-based compensation. Finally, a board is required to apply any recovery policy consistently to executive officers, and an issuer is prohibited from indemnifying any current or former executive officer for recovered compensation. The deadline for adoption of a compliant clawback policy was December 1, 2023.

Dodd-Frank

Under the Dodd-Frank Act, bank holding companies with total assets of $10 billion or more and certain other non-bank financial companies must have a separate risk committee that includes at least one risk management expert with experience managing risks of large companies.

III. OTHER SOURCES OF GUIDANCE ON OVERSIGHT

Department of Justice Guidance on the Design of Effective Compliance Programs

In recent years, DOJ leadership has placed increasing emphasis on the importance of an effective corporate compliance program in evaluating a company's culpability and eligibility for leniency in connection with investigations of corporate misconduct. That emphasis is reflected, for example, in the revised Corporate Enforcement Policy announced in January 2023, which underscores that an effective compliance program can mark the difference between a declination and a less favorable outcome—even where there are aggravating factors present.

These revised DOJ policies and accompanying policy statements put a premium on the thoughtful design and implementation of genuinely effective compliance programs. They also point to areas of particular DOJ interest to which boards should be attuned, including policies governing use and preservation of employees' business-related communications over all platforms and media and policies concerning compensation clawback.

Directors should consider borrowing from the DOJ's own guidance on compliance programs by constructively posing many of the same probing questions that the DOJ now expects federal prosecutors to ask. The DOJ guidance focuses on the same fundamental questions a well-

informed director should want to pose: Is the company's compliance program well designed, adequately resourced, drawing upon the right information and data, and effective at driving the right ethics and compliance messages throughout the organization? Management should be expected to provide the board or appropriate board committees with timely and complete answers to these kinds of questions, and do so periodically.

In keeping with DOJ's guidance, a compliance program should be designed by people with relevant expertise and will typically include interactive training as well as written materials. Compliance policies should be reviewed periodically to assess their effectiveness, to ensure they target the company's current compliance risks, and to make any necessary changes. Policies and procedures should fit with business realities. A rulebook that looks good on paper but which is not followed will hurt, not help. There should be consistency in enforcing stated policies through appropriate disciplinary measures. Finally, there should be clear reporting systems in place both at the employee level and at the management level so employees understand when and to whom they should report suspected violations and so management understands the board's or committee's informational needs for its oversight purposes. A company may choose to appoint a chief compliance officer and/or constitute a compliance committee to administer the compliance program, including by facilitating employee education and issuing periodic reminders. If there is a specific compliance area that is critical to the company's business, the company may consider developing a dedicated compliance apparatus for it.

Third-Party Guidance on Best Practices

Various industry-specific regulators and private organizations publish suggested best practices for board oversight of risk management. Example frameworks that have been used to inform internal enterprise risk management processes include guidance published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the "Three Lines Model" published by the Institute of Internal Auditors, ISO 31000 published by the International Organization for Standardization, and guidance periodically issued by the National Association of Corporate Directors (NACD) and the Conference Board.

In 2017, for example, COSO released its updated internationally recognized enterprise risk management framework. Recognizing that calls for identifying and mitigating ESG risks had become increasingly urgent, in 2018 COSO, in conjunction with the World Business Council for Sustainable Development, released guidance for applying enterprise risk management to ESG-related risks. COSO then issued supplemental guidance in March 2023 to help companies achieve effective internal control over sustainability reporting.

IV. CONTINUED STRONG INVESTOR FOCUS ON RISK MANAGEMENT

Institutional Investors

Risk oversight is a top governance priority of institutional investors. In recent years, investors have pushed for more meaningful and transparent disclosures on board-level activities and performance with respect to risk oversight. Growing investor pressure in this arena has prompted SEC rulemaking targeted at disclosures of climate and cybersecurity risks, as well as comment letters seeking additional risk disclosures in proxy statements. The pressure is also being

felt during the proxy season where institutional investors have lent their support to shareholder proposals calling for greater disclosures on a range of business, operational, human capital, environmental, social, and sustainability-related risks. Companies also increasingly include climate and other ESG-related risk disclosures in annual sustainability reports.

Major institutional investors such as BlackRock, State Street, and Vanguard, as well as actively managed funds, have expressed the view that sound risk oversight practices are key to enhancing long-term, sustainable value creation, and have emphasized oversight of sustainability-related risks, as well as other business risks. For example, in its 2024 proxy voting policy for U.S. portfolio companies, Vanguard stated that "[b]oards should take a thorough, integrated, thoughtful approach to identifying, quantifying, mitigating, and disclosing risks that have the potential to affect shareholder value over the long term."

Proxy Advisory Firms

In exceptional circumstances, scrutiny from institutional investors with respect to risk oversight can translate into shareholder campaigns and adverse voting recommendations from proxy advisory firms such as Institutional Shareholder Services (ISS) and Glass Lewis. Both ISS and Glass Lewis will recommend voting "against" or "withhold" in director elections—even uncontested ones—when the company has experienced certain extraordinary circumstances, including material failures of risk oversight.

In its 2024 Global Proxy Voting Guidelines, ISS states that it will, "[u]nder extraordinary circumstances, vote against or withhold from directors individually, committee members, or the entire board" for material failures of risk oversight. Examples of such failures include bribery, large or serial fines or sanctions from regulatory bodies; demonstrably poor risk oversight of environmental and social issues, including climate change; significant adverse legal judgments or settlements; or hedging of company stock. ISS has also focused attention on climate risk oversight failures, noting that it will vote against or withhold from the incumbent chair of the responsible committee (or other directors on a case-by-case basis) where it determines that the company is not taking the minimum steps needed to understand, assess, and mitigate risks related to climate change.

Glass Lewis's 2024 proxy voting guidelines likewise reflect increased scrutiny on board oversight of environmental and social risks. Glass Lewis expects to hold directors accountable where companies have "displayed disregard for environmental or social risks, have engaged in egregious or illegal conduct, or have failed to adequately respond to current or imminent environmental and social risks that threaten shareholder value" and will generally recommend voting against a governance committee chair of a company in the Russell 1000 that fails to provide disclosure concerning the board's role in overseeing environmental and social issues.

Proxy advisory firms, however, are cognizant of the range of investor perspectives with respect to ESG matters and have taken steps to afford their clients flexibility. In March 2023, ISS released a new set of Board-Aligned Proxy Voting Guidelines, which are designed to allow subscribing investors to uphold "foundational corporate governance principles as a means of protecting and maximizing their investments" while following board recommendations on environmental or social proposals.

V. RECOMMENDATIONS FOR IMPROVING RISK OVERSIGHT

The board should ensure that the company has mechanisms in place to encourage effective, ongoing communication with management, to design the right relationships across the board, its committees, management, and the workforce regarding risk oversight, and to monitor that the right level of resources support risk management systems, compliance, and reporting mechanisms. While risk management should be tailored to company risks, in general, an effective risk management system will: (1) adequately identify the material enterprise risks that the company faces in a timely manner; (2) adequately transmit necessary information to senior executives and to the board and/or relevant board committees; (3) implement appropriate risk management strategies that are responsive to the company's risk profile, business strategies, specific material risk exposures, and risk tolerance thresholds; (4) integrate consideration of risk and risk management into strategic and operational decision-making throughout the company; (5) feature regular reviews of the effectiveness of the company's risk management efforts, on a quarterly or semiannual basis; and (6) document risk management protocols and actions and board-level engagement on risk matters.

Specific Recommendations

Below are specific actions the board and appropriate board committees should consider as part of their risk management oversight:

- review with management the categories of risk the company faces, including any risk concentrations and risk interrelationships, as well as the likelihood of occurrence, the potential impact of those risks, mitigating measures, reporting and monitoring, and action plans to be employed if a given risk materializes;

- review with management the company's risk appetite and risk tolerance, its tools for measuring company-wide risks and assessing risk limits, and whether the company's business strategy is consistent with the agreed-upon risk appetite and tolerance, taking into account feedback from management and stakeholders;

- review with management the primary elements comprising the company's risk culture, including establishing a "tone at the top" that reflects the company's core values and the expectation that employees act with integrity and promptly escalate instances of noncompliance, and steps to ensure effective communication of and compliance with the company's risk management strategy throughout the enterprise and through appropriate public disclosures;

- review the company's director, executive, and employee compensation structure and incentive programs to ensure they are appropriate in light of the company's articulated risk appetite and that these programs are creating incentives to encourage, reward, and reinforce desired corporate behavior;

- review with committees and management the board's expectations as to each group's respective responsibilities for risk oversight and management to ensure a shared

understanding as to roles and accountability, including the quality, format, and cadence of management's risk reporting to the board and/or appropriate committees;

- review and reassess the allocation of board and committee oversight responsibilities with respect to the different categories of new and evolving risks the company faces, including consideration of whether to form ad hoc or subcommittees, where appropriate, to address particular risks; and

- review the skills and professional experiences that would best serve the board in overseeing the company's risk management, to assess whether the current board's mix of skills and professional experiences may benefit from supplementation (including through use of outside advisors), and to identify selection priorities to be used as part of the board recruitment and refreshment process.

The board should formally review, on at least an annual basis, the company's risk management system, including a review of board- and committee-level risk oversight policies and procedures and a presentation of "best practices" to the extent relevant, tailored to focus on the industry or regulatory arena in which the company operates. But because risk, by its very nature, is subject to constant and unexpected change, annual reviews cannot replace the need to regularly assess and reassess company operations and processes, learn from past mistakes and external events, and seek to ensure that current practices enable the board to address specific major issues whenever they may arise. Where a major or new risk event comes into focus, management should investigate and report back to the full board or the relevant committees as appropriate.

While fundamental risks to the company's business strategy are often discussed at the full board level, many boards continue to delegate primary oversight of risk management to the audit committee, which is consistent with the NYSE corporate governance standard requiring the audit committee to discuss risk assessment and risk management policies. In recent years, the percentage of boards with a separate risk committee has grown, but that percentage remains relatively low. According to a 2023 Spencer Stuart survey, only 12% of S&P 500 companies had a standing risk committee. As discussed above, companies subject to Dodd-Frank are required to have a dedicated risk committee. However, the appropriateness of a dedicated risk committee at other companies will depend on the industry and specific circumstances of the company. If the company keeps the primary risk oversight function within the audit committee, the audit committee should schedule periodic review of risk management outside the context of its role in reviewing financial statements and accounting compliance.

Thoughtfully allocating responsibility for risk management and compliance among the board's committees also creates an opportunity for alignment of officer-to-board-level reporting relationships, which has the added value of ensuring that the directors get to know and regularly communicate with a broader range of corporate executives. In an era in which the number of insiders on a company's board is usually just one or two—generally, the CEO and perhaps one additional director—board/management alignment gives the board direct insight into the company's operations and culture.

Any committee charged with risk oversight should hold sessions in which it meets directly with key executives primarily responsible for risk management. It may also be appropriate for the

committee(s) to meet in executive session both alone and together with other independent directors to discuss the company's risk culture, the board's risk oversight function, and key risks faced by the company. In addition, senior risk managers and senior executives should understand they are empowered to inform the board or committee of extraordinary risk issues and developments that require immediate board attention outside the regular reporting procedures. In light of the *Caremark* standards discussed above, the board should feel comfortable that it receives reports of red flags or "yellow flags," so that such issues may be investigated as appropriate.

VI. SPECIAL CONSIDERATIONS REGARDING ESG AND SUSTAINABILITY-RELATED RISKS

ESG risks have become a core area of risk oversight responsibility for the board. There is a growing consensus among investors and proxy advisors that ESG risks have the potential to significantly impact a company's long-term strategy and value creation, and consequently, boards need to oversee the monitoring, disclosure, and management of such risks. The range of stakeholders who may be interested and involved in ESG issues also presents unique challenges for boards who are increasingly tasked with using their business judgment to balance competing priorities across different time horizons.

The growing scale and intensity of ESG risks, particularly climate and nature-related risks, have increasingly drawn the attention of regulators at home and abroad. In 2021, the SEC announced the creation of the Climate and ESG Task Force in the Division of Enforcement, to focus on identifying misstatements in companies' disclosure of climate risks and gaps in existing disclosure requirements. The Task Force also analyzes disclosure and compliance issues relating to investment advisers' and funds' ESG strategies and has already undertaken enforcement actions resulting in sizeable settlements. The SEC's current rulemaking agenda also includes additional human capital and board diversity disclosures which seek to provide investors with greater insight into company risks and performance in these areas. SEC Chair Gary Gensler has stated that the recent proposed rulemaking is in line with the "core bargain from the 1930s . . . that investors get to decide which risks to take, as long as public companies provide full and fair disclosure and are truthful in those disclosures." Regulators abroad are taking similar action: the EU's Corporate Sustainability Reporting Directive (CSRD), which was formally adopted last year, will require companies operating in the EU (including over 3,000 U.S. companies) to identify and disclose how they are managing sustainability-related risks. Similarly, the UK's Financial Conduct Authority has passed measures requiring UK-listed companies to disclose in their annual financial reports climate-related risks aligned with the recommendations of the Task Force on Climate-related Financial Disclosures (TCFD) and standards adopted by the International Sustainability Standards Board (ISSB). Several jurisdictions, including Australia, Brazil, Canada, China, Singapore, and New Zealand, are also expected to adopt mandatory ESG disclosures similar to the standards prescribed by the ISSB.

Notwithstanding the significant investor and regulatory pressure for corporate transparency on ESG and sustainability risks, the past two years have also seen a wave of aggressive opposition from certain state legislatures and investors to corporate efforts to disclose and mitigate ESG risks. In August 2022, a coalition of 19 state attorneys general issued a letter to BlackRock admonishing it for its policies on climate change and ESG matters and alleging that its "past public commitments indicate that it has used citizens' assets to pressure companies to comply with international

agreements such as the Paris Agreement that force the phase-out of fossil fuels, increase energy prices, drive inflation and weaken the national security of the United States."

Several state legislatures, including Texas, West Virginia, Kentucky, Tennessee, Oklahoma and Florida, have also adopted new prohibitions on investment funds that have ESG mandates. Texas has banned 10 large banks and 348 investment funds for allegedly boycotting fossil fuel-based energy companies critical to the state's economy, while West Virginia has banned JPMorgan Chase, Wells Fargo, Goldman Sachs, Morgan Stanley, and BlackRock from doing business with the state due to their decisions to cut back on financing to coal companies. It remains unclear whether such bans will steer institutional investors away from efforts to address climate and other ESG risks: a study from the Wharton School indicates that the states may be paying the price for their policies, with Texas paying between $303 million and $532 million more in interest on the $32 billion it borrowed during the first eight months after the anti-ESG laws Texas enacted in 2021 took effect, and some large banks had to cease bond underwriting. However, the recent wave of backlash has quieted the public discourse on ESG, with some investors steering clear of the term entirely, and focusing instead on the underlying issues, namely risks to their portfolios.

In the wake of the Supreme Court's decision on affirmative action, there is an increasing level of scrutiny on companies' DEI initiatives, from both opponents and supporters. Companies are likely to face more questions from all sides over why and how they go about identifying, evaluating and implementing DEI policies and goals. Managing the tension between proponents and opponents of DEI programs and initiatives is particularly challenging because of the range of stakeholders involved. Shareholders, employees, customers, suppliers, regulators, stock exchanges, and state legislatures are among the groups that have sought to shape the DEI agenda. And DEI is not just a domestic issue: the EU's CSRD framework includes disclosure standards that require firms to assess and disclose workforce and supplier DEI policies, practices, and metrics to ensure equal treatment and opportunities for all.

Recommendations for Improving ESG Risk Oversight

The board's function in overseeing management of ESG-related risks involves issue-specific application of the risk oversight practices discussed in this guide. The board should work with management to identify ESG issues that are pertinent to the long-term sustainable value of the business (including taking into account and balancing the perspectives of the company's stakeholders) and oversee the policies and processes for identifying, assessing, monitoring and managing ESG risks. The board should be comfortable with the company's approach to external reporting and stakeholder engagement regarding the company's ESG strategy. It is increasingly important for directors and management who engage with shareholders and other stakeholders to be knowledgeable about the key ESG issues that affect or may affect the company. Some such issues may present opportunities to be factored into business strategy.

Below are specific considerations that the board and appropriate board committees should consider as part of their oversight of ESG risks:

- understand the material ESG risks relating to the company along with the company's progress, targets, goals, initiatives, and aspirations on ESG issues, recognizing that risks and opportunities continue to evolve;

- review the allocation of oversight responsibilities with respect to ESG matters on the board, including formalizing responsibilities among board committees and taking into account the respective capacities and existing functions of each board committee;

- where applicable, integrate ESG considerations into discussions on business strategy, broader risk management processes, and financial oversight;

- review and oversee the company's key ESG-related risk disclosures, including any ESG report and risk factor disclosures in the company's annual and quarterly reports filed with the SEC;

- review and assess management's monitoring and reporting processes with respect to ESG risks, including verification processes and internal controls, processes by which the board or board committee(s) discuss ESG matters with management, and the frequency of such discussions and whether there are ESG risk blind spots;

- assess how best to frame and describe ESG policies externally (including whether to use the term "ESG"), in light of the increasing polarization around ESG issues;

- periodically review the board's understanding of ESG issues, including whether the board would benefit from additional internal and external education and advisor assistance to ensure effective oversight; and

- ensure that monitoring and oversight of ESG disclosures, strategies, policies, commitments, and practices are properly documented in the board minutes and records.

VII. SPECIAL CONSIDERATIONS REGARDING CYBERSECURITY, RANSOMWARE, AND DATA PRIVACY RISKS

As businesses of all profiles become ever more dependent on technology and data management, cybersecurity risks have become increasingly salient. Indeed, failure to adequately identify, control, and mitigate cyber risk can be devastating. The events of recent years, which led the Biden administration to issue multiple Executive Orders declaring cyber threats a "top priority and essential to national and economic security," and to promulgate in 2023 a "National Cybersecurity Strategy" (and associated Implementation Plan), underscore this need. The risk of targeted attacks from criminal groups and state-sponsored malefactors has increased with the spread of remote or hybrid work arrangements, the embrace of cloud-based operations, the continued growth of virtual commerce, the proliferation of the Internet of Things, and the rapid development of AI tools. Incidents such as the May/June 2023 MOVEit "zero-day" attack by a Russian ransomware group, which affected some 668 business and governmental organizations (primarily in the United States) and involved the data of some 46 million individuals, underscore the imperative that companies diligently consider cybersecurity risks, mitigate vulnerabilities, engage in active and multi-layered defense, leverage law enforcement resources and third-party specialists identified in advance, plan for a robust and rapid incident response, and consider securing appropriate insurance coverage.

At the same time, legal and regulatory demands on companies to safeguard consumer data, protect against intrusions and make related disclosures to government agencies, stockholders, and the public have increased in recent years. The EU's General Data Protection Regulation (GDPR), which took effect in 2018, has transformed data handling obligations of companies whose operations have even a minimal European nexus, as has domestic legislation like the California Consumer Privacy Act and California Consumer Privacy Rights Act, the Virginia Consumer Data Protection Act, and the Colorado Privacy Act. While some states regulate biometric data as part of comprehensive privacy statutes, Illinois, Texas, and Washington have passed statutes that specifically regulate biometric data. Class action lawsuits brought under the Illinois statute against corporate defendants have resulted in settlements and damages awards in the hundreds of millions of dollars. Bills have been introduced in several state legislatures modeled on the Illinois statute.

Federal and state agencies have made cybersecurity a top focus. Of particular note, in July 2023, the SEC finalized wide-ranging cybersecurity-related disclosure rules for public companies first proposed in 2022. The final rules, which went into effect on September 5, 2023, require registrants to disclose on the new Item 1.05 of Form 8-K any cybersecurity incident within four business days after the registrant determines the incident to be material. Registrants are also required to disclose in their annual report on Form 10-K, pursuant to the new Regulation S-K Item 106, their processes for assessing, identifying, and managing material risks from cybersecurity threats, the material impacts of cybersecurity threats and previous cybersecurity incidents, the board's oversight of risks posed by cybersecurity threats, and management's role and expertise in assessing and managing material risks posed by cybersecurity threats.

The SEC has also taken numerous enforcement actions with respect to cybersecurity controls and the safeguarding of customer information, including a 2023 enforcement action charging SolarWinds and its chief information security officer with fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities, a 2023 settlement against Blackbaud relating to alleged misrepresentations around a ransomware attack and associated failure to maintain adequate disclosure controls, a 2022 settlement with Morgan Stanley Smith Barney relating to alleged failures (largely centered on alleged lax monitoring of vendors) to protect the personal identifying information of some 15 million customers, and a 2021 settlement with First American Financial Corporation for alleged failure to maintain disclosure controls and procedures sufficient to ensure that all available relevant information concerning a cybersecurity problem was analyzed for inclusion in the company's disclosures. These matters underscore that not only must companies maintain robust cybersecurity controls (including in respect of vendors), but they must implement procedures sufficient to provide reasonable assurance that, in a crisis, senior management receives accurate and timely information, with material updates in real time.

Other regulatory agencies have also been active on the cybersecurity enforcement front in recent years. For example, the DOJ in September 2023 announced a $4 million settlement with Verizon Business Network Services LLC resolving False Claims Act allegations that it failed to completely satisfy certain cybersecurity controls, and, in 2022, settled charges against Aerojet Rocketdyne that it had violated the False Claims Act by misrepresenting its cybersecurity compliance under certain federal government contracts. In June 2023, the Federal Trade Commission (FTC) settled charges against Microsoft in respect of the collection of personal information from minor users of the Xbox gaming system without parental consent. This

settlement is just the latest illustration of the FTC's increased activity in the data privacy and protection arena. Another agency that has been particularly active is the New York State Department of Financial Services (NYDFS), which has brought actions enforcing the detailed and prescriptive cybersecurity regulations it put in place in 2019 (and has continued to refine), including, for example, a May 2023 settlement with OneMain Financial Group relating to cybersecurity control failures.

Broadly speaking, the available regulatory and other guidance for cybersecurity risk management tracks the framework established by the National Institute of Standards and Technology (NIST), a critical benchmark that has been used and endorsed by the SEC and the FTC. The NIST elements are: identification of risk, protection of key data and systems, incident detection, incident response (including disclosure), and recovery. At the board level, the guidance is appropriately less operational and instead focused on ensuring that management is thinking about and addressing cyber risk in line with the company's risk profile and organizational goals and strategy. These principles are reflected, for example, in the NACD's 2023 Director's Handbook on Cyber-Risk Oversight.

VIII. CONCLUSION

Directors face a rapidly evolving risk and governance landscape, and boards are now recognized as having responsibility, as part of their oversight function, to use their business judgment working with management to assist in identifying material business and liability risks and to help articulate the strategy and the time horizon for mitigating these risks. Such expectations for board oversight have been reinforced by recent Delaware decisions that have turned on whether a company can point to documented processes for overseeing and responding to significant enterprise risks. In the face of an increasingly complex business environment fraught with new and sometimes unexpected risks, investors are looking to the board to take the lead on identifying, monitoring, and mitigating risks, including taking steps to work with management and advisors to adapt risk management processes to evolve with the evolving risk landscape and stakeholder expectations. Boards that take steps to implement and adhere to fit-for-purpose risk oversight processes will help play a critical role in protecting corporate reputation, engendering trust among shareholders, regulators, and other stakeholders, and ensuring long-term corporate health.

Martin Lipton
Daniel A. Neff
Andrew R. Brownstein
Steven A. Rosenblum
John F. Savarese
Adam O. Emmerich
David M. Silk
Wayne M. Carlin
William D. Savitt
David B. Anders
Karessa L. Cain
Sarah K. Eddy
Kevin S, Schwartz
Ryan A. McLeod
Anitha Reddy
Elina Tetelbaum
David M. Adlerstein
Carmen X. W. Lu
Raeesa I. Munshi
Anna M. D'Ginto
Kelley J. Merwin