Wachtell, Lipton, Rosen & Katz

Risk Management and the Board of Directors

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
Andrea K. Wahlquist
Karessa L. Cain
Sarah K. Eddy
Sabastian V. Niles
Ryan A. McLeod
Anitha Reddy
David M. Adlerstein
Carmen X. W. Lu
Raeesa I. Munshi
Cody Westphal

September 2022

Risk Management and the Board of Directors

I. INTRODUCTION

Overview

As companies seek to navigate a multi-stakeholder global landscape and the world continues to adjust to the impacts of Covid-19, significant new risks have emerged that are reshaping the near-term business and risk landscape. These new risks—and the intensification of longstanding risks—are pressure-testing the agility and resilience of corporate strategies, risk management systems and practices. The pandemic accelerated technological disruptions and business model changes and exposed sharp differences in the impacts felt by different sectors, with some experiencing enormous dislocation and others doing remarkably well and arguably emerging stronger. Looking ahead, all sectors of the economy are facing macroeconomic headwinds, including persistent inflation, surging interest rates, continued supply-chain bottlenecks and commodity shortages, all occurring amid the backdrop of the war in Ukraine, China's zero-Covid policy and growing geopolitical tensions. Severe drought, heatwaves and flooding across the globe have highlighted the burgeoning challenge of climate risks, which, along with the tight labor market and declining fertility rates across the developed world, present near- and longer-term risks that will require significant planning. Cybersecurity also continues to be a significant threat with regulators stepping up focus in step with growing geopolitical risks. In the United States, the 2022 midterms and ongoing political polarization continue to create uncertainties and surprises that companies will need to prepare for and address.

More than two-thirds of organizations surveyed by the American Institute of Certified Public Accountants ("AICPA") noted that perceived risk volumes and complexities remain elevated as companies across all sectors continue to deal with the litany of risks noted above. Surveyed organizations also recognized a "need for real change in how organizations govern business continuity and crisis management" in light of growing pressures from stakeholders for more disclosure about risks and heightened demands on management and boards to enhance effective risk management and preparedness for unexpected risk events. The World Economic Forum's Global Risks Report 2022 highlighted the economic and societal ramifications of the Covid pandemic, noting that domestic and global fragmentation may worsen the pandemic's impacts and complicate the coordination needed to tackle the challenges ahead.

The disparate and newly emerging risks facing companies today call for boards and management to reassess and update their organization's risk profile and vulnerabilities, evaluate the maturity and robustness of risk management processes and policies, and integrate risk management into strategic decision-making.

Managing corporate risk is not simply the business and operational responsibility of a company's management team—it is a governance issue that is squarely within the oversight responsibility of the board. Courts and regulators are increasingly scrutinizing the presence and effectiveness of board-level risk oversight systems, as well as the adequacy of public disclosures and quality of board responses when crises erupt. Recent *Caremark* decisions from the Delaware Court of Chancery have continued to influence the risk governance landscape. And

pressure is coming from other sources, including an emerging wave of "anti-woke" investors, state legislatures and state attorneys general campaigning for a rollback of recent efforts to address ESG-related risks, including climate change.

This guide highlights critical risk-management issues and provides updates on Delaware law governing director liability—including developments that highlight the importance of active, engaged board oversight of corporate risk and maintaining appropriate records of that oversight. Key topics addressed in this guide are:

- the distinction between risk oversight and risk management;
- tone at the top and corporate culture as components of effective risk management;
- recent developments in Delaware law regarding fiduciary duties and other legal frameworks;
- third-party guidance on risk oversight best practices;
- institutional investor focus on risk matters;
- specific recommendations for improving risk oversight;
- U.S. Department of Justice guidance on the design of compliance programs;
- special considerations pertaining to ESG and sustainability-related risks, including the emerging pushback from certain investors and state regulators; and
- special considerations regarding cybersecurity, ransomware and data privacy matters.

Risk Oversight by the Board—Not Risk Management

Both the law and practicality continue to support the proposition that boards cannot and should not be involved in day-to-day risk *management*. However, as recent legal developments make clear, 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; that these policies and procedures are functioning as directed; and that necessary steps are taken to foster an enterprise-wide culture that supports appropriate risk awareness, behavior and judgments about risk, and that recognizes and appropriately addresses risk-taking that exceeds the company's determined risk appetite. 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 formal committees may be necessary to focus oversight on particular risks. 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.

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

Covid-19 strained many companies and highlighted the critical importance of ensuring that the board and relevant committees 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. The lessons from the pandemic still ring true today where boards are expected to not only help steer companies through the complex economic environment, but also serve as a sounding board for the company's positioning on social and political issues of importance to the company's various stakeholders—employees, customers, suppliers and stockholders—whose views on these issues are not always aligned. 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. It is particularly important that the messaging from the board promptly adapts and responds to salient challenges; prolonged silence and/or board inaction to "get ahead" of key risks can harm a company's relationships with stakeholders and tarnish its reputation and brand image. This is particularly the case in a tight labor market that is transitioning to a new generation of employees and consumers who are scrutinizing corporate purpose and behavior. Cases in point include those instances where employee safety and well-being are concerned and at companies and industries where product or service failures can jeopardize consumer or environmental safety, critical infrastructure or human life. The 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. In the 2022 AICPA report, 44% of organizations cited competing priorities as a barrier to effective enterprise risk management.

Continued developments, including shareholder pressure to promote accountability and progress on diversity, equity and inclusion ("DEI") initiatives, also underscore the importance of setting the appropriate tone at the top. Discrimination and harassment can have a devastating impact both on the employees impacted by such behavior and on broader corporate culture, employee morale and retention, consumer preferences and the reputation of the company and its board and management personnel. Delayed or indecisive responses to sexual misconduct or gender or racial discrimination can often be as damaging to a company as the misconduct itself. Similarly, 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 participation of human resources officers, public relations advisors and legal counsel. 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, remedies and application 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

The evolution of risks has accelerated following the pandemic, requiring boards to take a more active approach in ensuring directors have the skills to effectively oversee a company's pressing and emerging risks. Edelman's 2022 Trust Barometer found that most surveyed respondents ranked business ahead of NGOs, the media and the government (which ranked last) to take leadership and address societal issues. The same survey reported that most respondents bought brands, chose their workplace and made investments based on their beliefs and values. Stakeholder perceptions of companies as social and political actors have influenced practices and approaches on board composition and refreshment and have expanded the substantive responsibilities of boards.

The National Association of Corporate Directors' report "Fit for the Future" published in 2019 noted that director recruitment continues to prioritize "classic skills and experiences," such as executive leadership and finance, while under 5% of directors have experiences in emerging focus areas such as human capital and cybersecurity. Today, the trend has begun to pivot in recognition that boards need to be educated and counseled to effectively deal with broader strategic and stakeholder imperatives, cybersecurity and significant ESG risks that could impact the company. Stakeholders, including key investors, regulators and third-party disclosure frameworks, are actively calling for companies to disclose the scope and nature of such expertise on their boards, in addition to enhancing functional corporate-level capabilities.

To prepare for such risks, boards must engage in director training to build on existing skills and leverage management and advisor expertise to develop deep working knowledge of key emerging issues. In addition, the recruitment of new directors will need to address any potential knowledge, skill and background gaps. While some companies may decide it is necessary to seek directors with climate, cybersecurity or human capital experience, many others may conclude that it is more appropriate to further educate existing board members. And as expectations around corporate involvement, leadership and activism grow, boards will also need to be prepared to assume a more public-facing role on key issues, including being prepared to engage 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. Recent Delaware decisions highlight the heightened expectations for a developed record of oversight on a variety of risks and the importance of making a good faith effort to put in place a compliance system designed to help ensure that their companies operate within the bounds of the law and

that their products, services, and operations do not cause harm to consumers, community members, or the environment.[1]

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 addressing director liability for the corporation's failure to comply with external legal requirements. Delaware courts in the *Caremark* line of cases have held that directors can be liable 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 culpable 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 shareholder claims alleging breaches of fiduciary duty by directors to proceed 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 accepted well-pled 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 or a failure by the company to come forward with books and records evidencing meaningful board-level oversight has 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*.

Last year, the Delaware Court of Chancery in *In Re The Boeing Company Derivative Litigation* permitted a *Caremark* duty-of-oversight claim to proceed against the directors of the Boeing Company after concluding that the complaint described a board that "complete[ly] fail[ed] to establish a reporting system for airplane safety." Emphasizing that meeting minutes gave little sign of director engagement with safety issues, the court credited allegations that the board had no committee charged with direct responsibility to monitor airplane safety, seldom discussed safety, and had no protocols requiring management to apprise the board of safety issues. The court further determined that Boeing's board "turn[ed] a blind eye to a red flag representing airplane safety problems," citing allegations that the directors

[1] Delaware courts in the *Caremark* line of cases have pointed to the absence of exculpatory documentation produced in response to a stockholder's inspection demand as evidence that the directors "face a substantial likelihood of liability" for "failing 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).

"treated the [first 737 MAX] crash as an 'anomaly,' a public relations problem, and a litigation risk, rather than investigating the safety of the aircraft."

By contrast, in *Firemen's Retirement System of St. Louis* v. *Sorenson*, the Court of Chancery dismissed a derivative claim seeking to hold the directors and officers of Marriott International liable for a data breach that affected millions of guests, concluding that the allegations failed to demonstrate that the directors had "completely failed to undertake their oversight responsibilities, turned a blind eye to known compliance violations, or consciously failed to remediate cybersecurity failures." The court also reaffirmed that "the difference between a flawed effort and a deliberate failure to act is one of extent and intent"—with a *Caremark* claim requiring the latter. The court did warn, however, that high risk of cybersecurity threats "increasingly call[s] upon directors to ensure that companies have appropriate oversight systems in place," and that "corporate governance must evolve to address" these risks. Earlier this year, the Court of Chancery further underscored the utility of board risk management and compliance structures when it dismissed breach of fiduciary duty claims against the board of NiSource in *City of Detroit Police and Retirement Sys.* v. *Hamrock* on the grounds that the company had a board-level committee specifically charged with addressing the core risks posed by its business—including the risks of explosion. Breach of fiduciary duty claims brought against the board of SolarWinds were also dismissed recently for similar reasons.

Whether such lawsuits lead to findings of liability will often turn on whether the targeted company can persuade a court that it had in place control and monitoring functions commensurate with the scope and scale of the potential risk. Once a *Caremark* claim survives a pleadings motion, however, it becomes a vehicle for extensive discovery and takes on substantial settlement value, even if not meritorious.

Ultimately, the events preceding oversight litigation illustrate that risk cannot be contained entirely. Corporate trauma can happen, even to the best-run companies, and courts can be expected to permit multiple avenues of litigation attack when it does. The best approach is for boards to undertake regular review of mission-critical corporate operations and developments affecting enterprise-level risk. As important, boards and their advisers should create a clear written record of their review and their vigilant response to any compliance risks that may emerge, such that inspecting stockholders and reviewing courts will have a fair picture of directors' work. Boards that institute and document such regular reviews will be in accord with best practices for corporate risk management. In the litigation context, boards will have a powerful answer, available at the pleading stage, if ever charged with neglecting their oversight duties.

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 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. Upcoming SEC rulemakings will likely continue to seek to expand expectations and disclosures concerning cybersecurity, climate change, human capital management and other ESG

and sustainability-related matters. Recent SEC comment letters issued to companies in Fall 2022 have asked for enhanced 2023 proxy statement disclosures by companies that would provide more company-specific detail on the board's role in risk oversight and the relationship between the board's leadership structure and risk management matters..

On a more granular level, the SEC requires companies to disclose in their annual reports "factors that make an investment in [a registrant's securities] speculative or risky." This expansive directive was until a few years ago accompanied by risk factor examples set forth in Item 503(c) of Regulation S-K (now Item 105), but the SEC eliminated those specific examples out of concern that they were encouraging "boilerplate" disclosures of limited value to investors. In August 2020, in furtherance of its "principles-based approach" to risk factor disclosure, the SEC adopted rule amendments to Item 105, noting that the amendments are designed to "result in risk factor disclosure . . . more tailored to the particular facts and circumstances of each registrant" and reduce use of "generic risk factors." Thus, companies must now disclose, in a concise and logical fashion, the most significant risks and explain how each factor affects the company's business and securities. In September 2021, the SEC released a sample letter with requests it may make of companies to ensure compliance with SEC guidance on climate-related disclosure, and the staff has proceeded to issue a number of climate-related comment letters in recent months, focusing on issues of climate risk disclosure and mitigation efforts.

The SEC earlier this year proposed amendments to Regulations S-K and S-X to require new climate-related risk disclosures. If adopted, the proposed rules would significantly expand upon the SEC's 2010 climate guidance, which called on companies to disclose material climate change-related risks and opportunities in their description of business, legal proceedings, risk factors, and MD&A. Certain aspects of the proposed climate rules have drawn extensive requests for scaling back and mixed commentary and so may be modified, and, if they are ultimately adopted by the SEC, they will likely face litigation challenges depending on the scope of the final rules. Nevertheless, well-managed companies should keep these proposals in mind, because they contemplate domestic and foreign issuers disclosing, in registration statements, annual reports and audited financial statements, information on board and management climate-related risk oversight and governance, material climate-related risks and opportunities over the short-, medium- and long-term, Scopes 1 and 2 greenhouse gas emissions, impact of climate-related events on line items of audited financial statements, and climate-related targets, goals and transition plans (if any). Accelerated and large accelerated issuers would also be required to provide third-party attestation on their Scopes 1 and 2 disclosures, and, in certain cases, their Scope 3 emissions over time. The proposed rules will, if adopted, generally be phased in over the three years beginning 2023 for large accelerated filers; "smaller reporting companies" would be exempted from Scope 3 disclosures. Notably, the requirement for climate-related line items in audited financial statements will come within the scope of a registrant's internal control over financial reporting. Climate-related disclosures within registration statements, including information filed in annual reports and incorporated by reference, will also be subject to liability provisions under the Securities Act of 1933 but will be afforded protections under the forward-looking safe harbors pursuant to the Private Securities Litigation Reform Act ("PSLRA") (except disclosures made in an initial public offering registration statement to which the PSLRA does not extend). Additionally, all material public climate-related disclosures are subject to the liability provisions of Section 10(b) and Rule 10b-5 of the Securities and Exchange Act of 1934.

Stock Exchange Rules

New York Stock Exchange ("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.

Dodd-Frank

The Dodd-Frank Act created new federally mandated risk management procedures principally for financial institutions, requiring bank holding companies with total assets of $10 billion or more, and certain other non-bank financial companies, to have a separate risk committee that includes at least one risk management expert with experience managing risks of large companies.

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 rise management ("ERM") 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, as well as guidance periodically issued by the National Association of Corporate Directors ("NACD") and the Conference Board.

In 2017, COSO released its updated internationally recognized enterprise risk management framework. The updated framework consists of five components: (1) Governance and Culture (the tone of the organization, which reinforces the importance of enterprise risk management and establishes oversight responsibilities for it); (2) Strategy and Objective-Setting (the integration of enterprise risk management into the organization's strategic plan through the process of setting strategy and business objectives); (3) Performance (the identification and assessment of risks that may impact achievement of strategy and business objectives); (4) Review and Revision (the review of the organization's performance, which allows for consideration of how well the enterprise risk management components are functioning and what revisions are needed); and (5) Information, Communication and Reporting (the continual, iterative process of obtaining information, from both internal and external sources, and sharing it throughout the organization).

Recognizing that calls for identifying and mitigating ESG risks have become increasingly urgent, COSO, in conjunction with the World Business Council for Sustainable Development, released guidance in 2018 for applying enterprise risk management to ESG-related risks. This guidance recognizes that companies "face an evolving landscape of environmental, social and governance (ESG)-related risks that can impact their profitability, success and even survival" and that such risks have "unique impacts and dependencies." Notably, the guidance reaches social-related risks encompassing stakeholder opposition, supply chain matters, human capital and labor-related issues and the complex area of maintaining "'social license' to operate." The guidance offers an enterprise risk management approach that runs from governance to risk identification and assessment through to communication and reporting. COSO is currently also developing supplemental guidance to its internal controls frameworks, with focus on sustainability reporting for internal decision-making and external public reporting.

COSO released additional guidance in November 2020 regarding the nexus between enterprise risk management and compliance risk management. The guidance aims to address management of risks related to adhering to specific laws and regulations, as well as adjacent risks related to compliance with professional standards, internal organizational policies and contractual obligations. Importantly, it acknowledges that compliance risks may arise not only from insider action—of directors, management and employees—but also third parties such as suppliers, outside sales representatives and contractors. COSO has also issued still more guidance on how to apply its enterprise risk management framework to emerging areas including guidance released in September 2021 to help organizations apply the COSO framework and principles to implement and scale artificial intelligence and guidance released in February 2022 to help companies manage enterprise risks in a fast-changing business environment.

In July 2020, the Institute of Internal Auditors ("IIA") released an update to its "Three Lines of Defense" model in risk management, now named the "Three Lines Model," to reflect a reorientation from defending against risk toward value creation and prospective risk management. Under the prior version of the model, (1) management control was the first line of defense, (2) various risk control and compliance oversight functions established by management were the second line of defense, and (3) independent assurance was the third line of defense. The updated model incorporates the governing body, typically the corporate board, and makes it accountable to stakeholders for organizational oversight. In addition, the model's departure from the strict "three lines" approach highlights the need for collaboration and communication between the governing body, management and internal audit functions.

In early 2018, the International Organization for Standardization released an update to ISO 31000, an international standard that provides widely applicable guidelines and principles for risk management for a range of organizations. The risk management framework is composed of five areas—integration, design, implementation, evaluation and improvement—and centered around a sixth area, leadership and commitment involving senior management and oversight bodies. The principles of ISO 31000, which provide guidance on the characteristics of effective and efficient risk management and serve as the foundation of managing risk, include: continual improvement, integrated, structured and comprehensive, customized, inclusive, dynamic, best available information, and human and cultural factors. And ISO 31000's risk management process involves the systematic application of policies, procedures and practices to

the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

COSO, IIA and ISO 31000, as well as other frameworks outlining risk-related best practices, underscore that risk oversight and risk management should not be treated as isolated, defensive functions, but rather should be proactively integrated into strategic planning and prioritized as part of board- and CEO-level governance and oversight.

III. 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. As noted in the NACD's Blue Ribbon Commission report on disruptive risks, investors "keep raising the bar for boards on the oversight of everything from cybersecurity to culture, and the notion of companies' license to operate is now front and center." The growing investor pressure in this area has prompted SEC rulemaking specifically targeted at addressing climate and cybersecurity risks and comment letters to companies seeking clarity on the scope and rationale behind climate risk disclosures. 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 material, business, operational, human capital, environmental, social and sustainability-related risks.

Major institutional investors such as BlackRock, State Street and Vanguard, as well as actively managed funds, believe that sound risk oversight practices are key to enhancing long-term, sustainable value creation, and have emphasized oversight and monitoring of sustainability-related risks, as well as other business risks. BlackRock has stated that it "look[s] to the board to articulate the effectiveness of these mechanisms in overseeing the management of business risks and opportunities and the fulfillment of the company's purpose." Specifically, BlackRock expects boards to oversee the identification and management of material business operational, and sustainability-related risks and the robustness of a company's ERM framework as well as address business issues, including environmental and social risks and opportunities, when they have the potential to materially impact the company's long-term value, and may vote against directors that it deems responsible for particular inadequacies.

State Street has likewise stated that it believes the primary responsibility of the board is to preserve and enhance shareholder value and protect shareholder interests. State Street expects boards to monitor the risks that arise from a company's business, including with respect to sustainability, and has noted that "good corporate governance necessitates the existence of effective internal controls and risk management systems, which should be governed by the board." An area of specific focus is risks relating to DEI, which State Street expects companies to "effectively manage and disclose." For S&P 500 companies, State Street will act against the chair of the nominating committee if a company does not disclose the gender, racial and ethnic composition of its board or have at least one director from an underrepresented community. In addition, State Street has also developed its proprietary R-Factor scoring system which encourages companies to manage and disclose material, industry-specific ESG risks and which

State Street uses to determine whether to take voting action against the lead independent director of companies it deems "laggards."

Vanguard has said that it views directors as "responsible for effective oversight and governance of their companies' most relevant and material risks." In its 2022 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." Vanguard also expects boards to communicate their approach to risk oversight to shareholder through their normal course of business. Vanguard will vote against a director or committee for "material risk oversight failures," including failures regarding climate risk oversight.

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 in uncontested elections, when the company has experienced certain extraordinary circumstances, including material failures of risk oversight.

In its 2022 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 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 to the company and the larger economy. Such minimum steps include providing disclosures aligned with the recommendations of the Task Force on Climate-related Financial Disclosures and setting GHG emissions reduction targets. ISS's voting policies will also generally vote in favor of shareholder proposals seeking risk disclosures on a broad range of topics. The ISS ESG Governance QualityScore—a data-driven scoring and screening tool that ISS and other institutional investors use to monitor portfolio company governance—also focuses heavily on boards' audit and risk oversight.

Glass Lewis revised its proxy voting guidelines to reflect its increased scrutiny on board oversight of environmental and social risks. Glass Lewis believes that "the board's role is to ensure that management conducts a complete risk analysis of company operations, including those that have material environmental and social implications." 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." Risk areas that Glass Lewis believes necessitate management and oversight include environmental, social, regulatory, legal, reputation and governance. In addition, Glass Lewis has specifically noted

legal and reputational risks arising from poor conduct in foreign countries (such as bribery), gender pay inequity, human rights practices across the supply chain and issues arising from privacy, censorship, and freedoms of expression and access, and on a case-by-case basis will support shareholder proposals requesting further disclosures and action in these areas.

IV. RECOMMENDATIONS FOR IMPROVING RISK OVERSIGHT

The board should promote an effective, ongoing risk dialogue with management, design the right relationships across the board, its committees, management, and the workforce regarding risk oversight, and ensure that appropriate resources support risk management systems, compliance, and reporting mechanisms. While risk management should be tailored to the specific company and relevant risks, in general, an effective risk management system will: (1) adequately identify the material risks that the company faces in a timely manner; (2) adequately transmit necessary information to senior executives and, importantly, to the board 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 strategy development and business 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 the existence of risk management protocols and appropriate 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 management monitoring and reporting processes, including whether these processes are sufficiently robust and holistic to encompass the company's most critical risks and whether there are internal silos of risks impacting particular aspects of the business that could coalesce into enterprise-wide issues;

- 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 from 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 the company's risk management strategy throughout the organization 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, professional experiences and practices that are required by the board to effectively oversee risks, to assess whether the current board's mix of skills and professional experiences are sufficient and 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. In the wake of the recent Delaware decisions green-lighting *Caremark* claims across a variety of industries, directors should also implement effective procedures to ensure that the board itself monitors key enterprise risk on an ongoing basis and properly documents this monitoring. To this end, it may be appropriate for boards and committees to engage outside consultants to assist them both in the review of the company's risk management systems and in understanding and analyzing business-specific risks. 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 2021 Spencer Stuart survey, only 12% of the companies surveyed had a standing risk committee. As discussed above, companies subject to Dodd-Frank are required to have a dedicated risk management 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. The potential for overload is real: a Deloitte survey of U.S. public companies found that 32% of audit committee respondents expect to spend more time on ERM risk oversight this coming year while also noting that committee responsibilities have expanded to encompass oversight of ESG reporting and disclosures.

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.

Department of Justice Guidance on the Design of Effective Compliance Programs

As noted above, senior management should provide the full board or a relevant committee with an appropriate review of the company's legal compliance programs and how they are designed to address the company's risk profile and detect and prevent wrongdoing. While compliance programs should be tailored to the company's specific needs, the board and senior management of any company should establish a strong tone at the top that emphasizes the company's commitment to full compliance with legal and regulatory requirements, as well as internal policies.

This goal is particularly important not only to reduce the risk of misconduct, but also because a well-tailored compliance program and a culture that values ethical conduct are critical factors that DOJ will assess in considering whether to bring charges against a corporation in the event that corporate personnel engage in misconduct. Under the Principles of Federal Prosecution of Business Organizations, prosecutors are required to weigh, among other factors, the seriousness of the offense, the role (if any) of high-level management, the effectiveness of a company's compliance program at the time of the offense, the extent of cooperation and reporting, remedial measures taken and potential collateral consequences for innocent stakeholders. In addition, under DOJ's FCPA Corporate Enforcement Policy, which serves as non-binding guidance in all Criminal Division corporate fraud investigations, a company is eligible for an exercise of prosecutorial discretion in the company's favor—including a

declination of any prosecution—only if it has implemented an effective ethics and compliance program.

Late last year, DOJ announced an array of policy revisions that directly bear upon how boards and senior executives should manage risk. These announcements built upon updated guidance from June 2020 for white-collar prosecutors, which identified factors to be considered in evaluating corporate compliance programs, noting that prosecutors may "reward efforts to promote improvement and sustainability" of compliance programs in the form of any prosecution or resolution. DOJ further emphasized the need for a dynamic compliance program that makes use of data analytics and testing to review and address potential gaps in a company's compliance functions. In a major policy speech in October 2021, Deputy Attorney General Lisa Monaco announced that white-collar prosecutors would be encouraged to favor the imposition of a corporate monitor "[w]here a corporation's compliance program and controls are untested, ineffective, inadequately resourced, or not fully implemented at the time of a resolution" of a criminal investigation. To avoid the imposition of a monitor, companies should ensure that their "compliance program and controls are demonstrated to be tested, effective, adequately resourced, and fully implemented at the time of a resolution." These revised DOJ policies put a premium on the thoughtful design and implementation of genuinely effective compliance programs.

Directors should consider borrowing from the updated DOJ guidance by constructively posing many of the same probing questions that DOJ now expects federal prosecutors to ask. Those DOJ directives are aimed at understanding the same fundamental questions a well-informed director should want to understand: 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.

V. 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.

Heightened investor focus on ESG risks has also drawn the attention of regulators at home and abroad. On March 4, 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 will analyze disclosure and compliance issues relating to investment advisers' and funds' ESG strategies. This year, the SEC has released proposed rules specifically targeting the disclosure of climate-related and cybersecurity risks and has also issued comment letters to companies requesting clarification regarding their climate-related risk disclosures. The SEC's rulemaking agenda also includes additional human capital and board diversity disclosures that are slated to be released later this year or early next year, with a view to providing investors with greater insight into risks and performance in these areas. SEC Chair Gary Gensler has noted 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 also taking similar action: the EU's Corporate Sustainability Reporting Directive will require companies operating in the EU (including certain subsidiaries of foreign companies) to identify and disclose how they are managing sustainability-related risks, while 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.

Notwithstanding the significant investor and regulatory pressure for corporate transparency on ESG and sustainability risks, there is also a growing wave of pushback from certain state legislatures and investors against efforts to disclose and mitigate ESG risks. In August, 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." State legislatures in 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 July 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 they 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. Moreover, the institutions targeted by

these bans are frequently subject to other conflicting ESG-related laws, including foreign laws and to similar pressure from other stakeholders on these topics.

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 business and its stakeholders and decide what policies and processes are appropriate for assessing, monitoring and managing ESG risks, as well as how to incentivize proper management of these risks. The board should also be comfortable with the company's approach to external reporting and shareholder engagement regarding the company's overall approach, response and progress on ESG issues. And it is increasingly important for directors and management who engage with shareholders to educate themselves and become conversant on the key ESG issues facing the company. Companies are also wise to assess whether there are ESG-related 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 their company along with the company's progress, targets, goals, initiatives and aspirations on ESG issues, recognizing that materiality as it applies to ESG continues 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;

- integrate ESG considerations, where applicable, 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 discuss ESG matters with management and the frequency of such discussions and whether there are ESG risk blind spots;

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

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

Cybersecurity increasingly has become a risk factor that requires special attention—both because it affects all aspects of most businesses and because failure to adequately identify, control and mitigate cyber risk can be devastating. The events of the 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," underscore this need. The risk of targeted attacks from criminal groups, foreign intelligence services and other bad actors has increased with the mass shift to remote work arrangements, embrace of cloud-based operations, increased reliance on virtual commerce spurred by the pandemic, and the proliferation of the Internet of Things. CEOs surveyed by PwC for its 25th Annual Global CEO Survey ranked cyber risks as the top threat to growth, as evidenced by (among many other examples) the attacks on the Colonial Pipeline and on SolarWinds. Geopolitical tensions have augmented cybersecurity risks—in March 2022, President Biden issued a public warning that Russia was considering conducting cyberattacks against U.S. entities and U.S. critical infrastructure, as part of Russia's response to Ukraine-related sanctions. This risk came to fruition in the January 2022 destructive malware operation targeting multiple organizations in Ukraine, and in a crippling cyberattack against Toyota following Japanese condemnation of Russia's invasion of Ukraine. Incidents such as these 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 ("CCPA") of 2020 and the Virginia Consumer Data Protection Act of 2021.

Federal and state agencies have made cybersecurity a focus, bringing attention-grabbing enforcement actions for failure to abide by their overlapping webs of requirements. In November 2020, a little over a year after its historic data privacy settlement with Facebook, the Federal Trade Commission ("FTC") announced a settlement with Zoom for alleged misrepresentations to consumers about encryption levels and vulnerability of its software to remote video surveillance. This settlement is just one illustration of the FTC's increased enforcement activity in the data privacy and protection arena—a trend likely to persist despite a recent Supreme Court decision cutting back the agency's ability to pursue disgorgement and restitution remedies. Another agency that has been particularly active of late 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.

There is a silver lining to the twin pressures of increased cyber risk and accompanying regulatory focus: more sophisticated and nuanced guidance to companies about

cybersecurity risk oversight, management and disclosure. For example, the U.S. Department of the Treasury, Office of Foreign Assets Control ("OFAC") and Financial Crime Enforcement Network in October 2020 issued advisories to assist in combating ransomware attacks and to comply with sanctions and anti-money laundering regulations. In February 2021, NYDFS issued two guidance memos, one addressing cyber insurance, and another recommending steps that entities with public-facing websites should take to prevent unauthorized access to nonpublic information.

The SEC, for its part, has had cybersecurity interpretive guidance in place since 2011, requiring companies to "disclose the risk of cyber incidents if they are among the most significant factors that make an investment in the company speculative or risky." That guidance was clarified in 2018, and was supplemented in early 2020 by the Office of Compliance Inspections and Examinations' Cybersecurity and Resiliency Observations. But in recent proposed rulemakings, the SEC has taken an even more active role in cybersecurity. In February 2022, it proposed cybersecurity rules for registered investment advisers and funds, and for public companies, with complementary rules for registered broker-dealers and other market intermediaries forthcoming. The proposed rules for registered investment advisers and funds encompass cybersecurity risk management policies and procedures, enhanced disclosure of cybersecurity risks and incidents, and recordkeeping requirements. The proposed rules for public companies also address both cybersecurity incident disclosure and cybersecurity policies and procedures, but add requirements for disclosure of director and management expertise. While the rulemakings are not final, all affected organizations should assess their current cybersecurity-related policies and procedures to identify and address any notable gaps between existing approaches and SEC expectations.

The SEC has also taken enforcement action on the cybersecurity front, such as a 2021 settled administrative order with Pearson plc, finding violations of the negligence-based antifraud provisions of the Securities Act and imposing a civil penalty after the company failed to disclose a major breach and responded to press inquiries by downplaying the breach, and in 2021 announced settled charges against First American Title Insurance Company for 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 actions underscore that disclosure decisions concerning cybersecurity incidents must be grounded in a full understanding of all material facts. If a company chooses to make a public statement, it must be accurate and not misleadingly incomplete. Further, companies cannot limit risk-factor language to boilerplate if they have experienced a major undisclosed cyber breach involving significant exposure of sensitive data.

Given the uptick in recent years in ransomware attacks—installation of malware that encrypts business data in an effort to extort ransom, usually in the form of cryptocurrency—against companies across various industries (such as the Russian-originated NotPetya attack which caused some $1.4 billion in damage to a global pharmaceutical company), the White House, in June 2021, issued an open letter to the private sector encouraging corporate leaders to view the specter of a ransomware attack as a direct threat to core business operations. The letter recommended that executives immediately convene their leadership teams to ensure that cyber defenses, as well as incident response, continuity and recovery plans were tailored to the evolving risk landscape. Later the same month, NYDFS issued guidance describing a number of

ransomware prevention measures that NYDFS-regulated entities should integrate into existing cybersecurity programs. In 2020, OFAC promulgated guidance that ransomware payments may violate OFAC regulations.

Broadly speaking, the available regulatory and other guidance 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 April 2021 Board Cybersecurity Oversight Guidance issued by the World Economic Forum ("WEF"), the National Association of Corporate Directors and the Internet Security Alliance, in partnership with PwC, and in the WEF's May 2021 white paper titled "Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers."

In general, the applicable guidance and our experience inform the following takeaways with respect to cyber risk:

- Oversight Mechanism: Boards should carefully consider with management the avenues through which they monitor cyber risk. Although it is common to delegate cyber risk oversight to the audit committee, this should be carefully considered given the burden on audit committees. An alternative is the formation of a dedicated, cyber-specific board-level committee or sub-committee. At the same time, because cybersecurity considerations increasingly affect all operational decisions, they should be a recurring agenda item for full board meetings. Companies that already have standalone risk or technology committees should also consider where and how to situate cybersecurity oversight. The appointment of directors with technology experience should be evaluated alongside director education.

- Review of Policies, Procedures & Resources: In carrying out their oversight function, directors should ensure that the company has written policies and procedures in place governing each of the NIST elements, and that both the cybersecurity and the internal audit functions include technical expertise and sufficient time and resources to devote to cybersecurity risk and review. A review of the common elements of remedial and other cyber-related enforcement actions suggests a growing expectation among regulators that companies maintain written information security programs that senior management present to the board at least annually.

- Verification of Risk Identification & Assessment: Directors should have a working understanding of the company's systems, and the data it collects, as well as the risks posed by how the company uses technology and collects and stores data. While managing the cybersecurity-related risks of remote work is a task that virtually every company has taken on as a result of the pandemic, each company's cyber risk profile is unique. The role of directors is to ensure that an effective cyber risk assessment and mitigation system is in place, that those managing the company's cybersecurity

identify and consider potential vulnerabilities (leveraging the latest threat intelligence and best practices) and that the board is engaged in active oversight of such matters.

- Oversight of Protection & Detection Strategies: Directors should be briefed on management's plan for protecting against cyber intrusions and related risks, including programmatic efforts to detect and mitigate vulnerabilities and enable business continuity. In addition, directors and executives should maintain a sustained focus on the timely remediation of material cyber risks, whether identified by internal or external sources, and, where appropriate protective or remedial recommendations are promptly implemented in response to identified exposures. Responsible personnel should engage in continuous monitoring and improvement efforts, including as to prosaic but mission-critical tasks like timely patching of critical systems, prompt installation of third-party software updates, and attentiveness to relevant industry bulletins (such as those released by the U.S. Cybersecurity & Infrastructure Security Agency). Knowledgeable employees from the internal audit function should usually be involved as well.

- Oversight of Response Strategy and Disclosure Protocols: Directors should receive briefings from time to time on management's protocols for a swift, robust and effective response to a breach or other cybersecurity incident, as well as on the company's response to material cybersecurity incidents and related impacts. A company's response plan should cover all likely incident scenarios, as well as plausible scenarios with extreme consequences. The plan should address notification and response protocols, procedures for escalation to appropriate management personnel and ultimately the board, business and service interruption scenarios (including whether systems could or should be taken offline as a precautionary measure) and communications with regulators and stakeholders. The company should also have a coherent and legally vetted plan for making appropriate and compliant disclosures and notifications to law enforcement, industry-specific regulators, consumers, and the public if and when data or other systems are materially compromised. Occasional "fire drills" should be considered.

- Documentation of Board-Level Oversight: Finally, board and committee oversight activities, including in the aftermath of a material cyber incident that causes significant harm or disruption, should be appropriately documented in minutes and in supporting materials. Shareholder books and records inspection demands in preparation for litigation are increasingly common and allowed by the courts where certain pleading requirements are met.

VII. CONCLUSION

Anticipating Future Risks

Understanding risks inherent in the company's strategic plans, risks arising from the competitive landscape and potential for technology and other developments to impact the company's profitability and prospects for sustainable, long-term value creation is critical to effective board-level risk oversight. Gaining that understanding, of course, will allow boards and

management to anticipate future risks, which, in turn, is critical to avoiding or mitigating those risks before they escalate into crises.

As stressed in the NACD's report, "Fit for the Future," boards are entering a time of both extreme challenge and promise:

> *The accelerating pace and intensifying complexity of change are leading to the emergence of a fundamentally different operating reality than incumbent executives and directors have experienced in their careers to date. However, this dizzying amount of change also creates immense opportunities for companies to out-innovate the competition, to generate value in new ways, and to strengthen their governance.*

The Road Ahead

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 wake of the pandemic and growing macroeconomic uncertainty and geopolitical instability, investors are increasingly 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 changing 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.

INDEX