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
Wayne M. Carlin
William D. Savitt
Sabastian V. Niles
Ryan A. McLeod
Anitha Reddy
Marshall L. Miller
Carol Miller
Monica M. Heinze
Raeesa I. Munshi

November 2019

Risk Management and the Board of Directors

I. Introduction

Overview

The risk oversight function of the board of directors has never been more critical and challenging than it is today. Rapidly advancing technologies, new business models, dealmaking and interconnected supply chains continue to add to the complexity of corporate operations and the business risks inherent in those operations. The evolving political environment further exacerbates the risks that corporations face. Corporate behavior has been blamed for accelerating environmental degradation and aggravating disparities in income and wealth. In addition, safety scandals and product failures have affected public confidence in the ability of corporations to manage business risk and have given rise to skepticism as to whether companies are sufficiently prioritizing consumer and product safety. Environmental, social, governance and sustainability-related issues have become mainstream business topics, encompassing a wide range of issues including business model resilience, employee wages, healthcare, training and retraining, income inequality, supply chain labor standards and corporate culture, as well as climate change. The reputational damage to companies, boards and management teams that fail to properly manage risk is substantial.

Within this broader context, corporate risk-taking and the monitoring of corporate risk remain top of mind for boards of directors, investors, legislators and the media. Companies should exercise care to address business risks and ESG issues, avoid public relations crises and develop and maintain reputations as responsible economic actors. Major institutional shareholders and proxy advisory firms routinely engage companies on risk-related topics and increasingly focus on risk oversight matters when evaluating corporate performance, including in proxy contests and when considering withhold votes in uncontested director elections.

Risk management is not simply a business and operational responsibility of management—it is a governance issue that is squarely within the oversight responsibility of the board. Directors face a risk governance landscape that continues to evolve, and this memorandum highlights a number of issues that have remained critical over the years. It also provides updates reflecting emerging and recent developments, including recent Delaware cases regarding risk oversight director liability—*Blue Bell* and *Clovis*—which highlight the importance of active, engaged board oversight of corporate risk as well as a record of that oversight. Key topics addressed in this memorandum include:

- the distinction between risk oversight and risk management;
- tone at the top and corporate culture as key components of effective risk management;
- recent developments in Delaware law regarding fiduciary duties and other legal frameworks;
- third-party guidance on best practices;

- the strong institutional investor focus on risk matters;
- specific recommendations for improving risk oversight;
- legal compliance programs;
- lessons from Wells Fargo on risk oversight;
- special considerations pertaining to ESG and sustainability-related risks;
- special considerations regarding cybersecurity matters; and
- anticipating future risks and the road ahead.

Risk Oversight by the Board – Not Risk Management

Both the law and practicality continue to support the proposition that the board cannot and should not be involved in day-to-day risk *management*. However, as recent legal developments in 2019 make clear, it is important that the board's role of risk *oversight* include steps taken at the board level, rather than solely at the management level, to be actively engaged in monitoring key corporate risk factors, including through appropriate use of board committees. It is also important that these board-level monitoring efforts 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. 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 risk appetite; 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, behaviors and judgments about risk, and that recognizes and appropriately addresses risk-taking that goes beyond the company's determined risk appetite. This necessitates that the board itself is kept aware of the type and magnitude of the company's principal risks, especially concerning "mission critical"-related areas, and is periodically apprised of the company's approach for mitigating such risks, instances of material risk management failures and action plans for mitigation and response. In prioritizing such matters, the board can send a message to management and employees that comprehensive risk management is not an impediment to the conduct of business nor a mere supplement to a firm's overall compliance program, but is, instead, an integral component of strategy, culture and business operations.

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

The board and relevant committees should work with management to promote and actively cultivate a corporate culture and environment that meets the board's expectations and is aligned with the company's strategy. Respecting the importance of enterprise-wide risk management is a valuable component of an effective corporate culture. 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 and avoiding compliance failures, and this commitment should be communicated effectively throughout the organization. In addition, particularly at companies and in industries where product or service failures can jeopardize consumer safety or threaten human life, the corporate culture should not, deliberately or due to inattention or insufficient resource allocation, prioritize cost-cutting or profits over safety and compliance.

Continued developments regarding sexual and other misconduct in the workplace make clear that setting the appropriate "tone at the top" is perhaps more important than ever before. Harassment can have a devastating impact, first and foremost, on the employees targeted by such predatory behavior. It can also have a significant impact on corporate culture, employee morale and retention, consumer preferences and public perception. In light of heightened media and public scrutiny, delayed or indecisive responses to sexual misconduct can often be as damaging to a company as the misconduct itself. Despite the serious risks associated with sexual harassment, many boards are still not adequately addressing whether they have the right policies and procedures in place to prevent sexually inappropriate behavior and/or sexism in the workplace. As revealed in a 2017 survey of 400 private and public company directors by Boardlist and Qualtrics, 88% of boards "had not implemented a plan of action as a result of recent revelations in the media," and 83% had not "re-evaluated the company's risks regarding sexual harassment or sexist behavior at the workplace." In a 2018 update, Boardlist and Qualtrics reported that more recent numbers "reflect steps in the right direction," but 57% of boards still had not discussed sexual harassment or sexist behavior at the workplace at all.

It is important that the board consider its oversight role with respect to sexual harassment claims and be briefed on the factors used by management in determining which claims are reported to the board. The board should review the company's policies and procedures regarding sexual harassment or assault allegations, and may want to be briefed on the company's employee training program and protocols for addressing sexual misconduct. The board should also work with management to consider developing a crisis response plan that includes the participation of human resources, public relations and legal counsel. The use, scope and design of preventative corporate policies regarding conduct and reporting should also be carefully considered, including as to potential implications, enforcement, remedies and application in the event of a violation once such policies are adopted.

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

In addition to heightened expectations from institutional investors, legislators and other constituencies, a board's risk oversight responsibilities derive from state law fiduciary duties, federal and state laws and regulations, stock exchange listing requirements and certain established (and evolving) best practices.

Fiduciary Duties

The Delaware courts have taken the lead in formulating the national legal standards for directors' duties for risk management, particularly following *In re Caremark International Inc. Derivative Litigation*, the seminal 1997 case 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 systemic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists," noting that this is a "demanding test." Delaware Court of Chancery decisions in the twenty years following *Caremark* regularly dismissed shareholder suits claiming such a total failure of oversight responsibility. See, for example, our memos discussing *In re Citigroup Inc. Shareholder Derivative Litigation* (2009), *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).

Recent rulings, however, indicate that the risk of exposure is real. *In re Wells Fargo & Company Shareholder Derivative Litigation*, decided in 2017, tested the limits of the *Caremark* doctrine. There, a California federal court applying Delaware law denied the defendants' motion to dismiss because the plaintiffs pointed to numerous "red flags" of which the company's directors allegedly were or should have been aware and took no substantial remedial steps. The plaintiffs asserted that Wells Fargo's directors knew or consciously disregarded that Wells Fargo employees were creating millions of deposit and credit card accounts for customers without the customers' knowledge or consent. The court rejected defense efforts to explain away the alleged red flags as "insignificant when viewed in their larger context." Rather than look at the red flags in isolation, as the defendants urged, the court viewed them collectively, finding that "Defendants ignore the bigger picture by addressing each of these 'red flags' in piecemeal fashion." The court concluded that while the red flags might "appear relatively insignificant to a large company like Wells Fargo when viewed in isolation, when viewed collectively they support an inference that a majority of the Director Defendants consciously disregarded their fiduciary duties despite knowledge regarding widespread illegal account-creation activities, and . . . that there is a substantial likelihood of directors oversight liability."

In June 2019, the Delaware Supreme Court reversed the Court of Chancery's dismissal of a *Caremark* suit. *Marchand* v. *Barnhill* (better known as "*Blue Bell*") arose from Blue Bell Creameries' distribution of ice cream tainted with listeria. The contaminated food killed three people, and the company had to recall its products and suspend operations. Plaintiffs sued to recoup their investment losses after the company engaged in a dilutive transaction to avoid insolvency.

The Delaware Supreme Court suggested that the existence of management-level compliance programs is not enough, standing alone, for directors to avoid *Caremark* exposure. The court observed that, while Blue Bell had certain food safety programs in place and "nominally complied with FDA regulations," it "had no [board] committee overseeing food safety, no full board-level process to address food safety issues, and no protocol by which the board was expected to be advised of food safety reports and developments." This "dearth of any board-level effort at monitoring" the company's risk management supported an inference that the directors had breached their oversight obligations. To "satisfy their duty of loyalty," the court held, "directors must make a good faith effort to implement an oversight system and then monitor it" themselves.

In October 2019, the Delaware Court of Chancery further extended the practical reach of the *Caremark* doctrine, upholding claims in *In Re Clovis Oncology, Inc. Derivative Liti-*

gation against directors of a life sciences firm for failing to ensure accurate reporting of drug trial results.

Clovis's stock dropped sharply in 2015 when it disclosed poor clinical trial results for its most promising experimental cancer drug. Federal securities actions challenging the company's previous disclosures about the drug and a related SEC investigation followed, and were settled. Shareholders then brought a derivative action alleging that the board breached its fiduciary duties by disregarding red flags that reports of the drug's performance in clinical trials were inflated.

The Court of Chancery recognized that the board had implemented robust reporting procedures regarding drug development and regularly received reports of the new drug's progress in clinical testing. Crediting allegations that the directors ignored "warning signs that management was inaccurately reporting [the drug's] efficacy," however, the court nevertheless sustained the claims. The Clovis directors argued, and the court accepted, that duty-to-monitor claims require a showing of scienter—that is, evidence that the directors knew they were violating their duties. But the court did not require the plaintiff to allege particular facts showing such knowledge. Instead, reasoning that Clovis had a board "comprised of experts" and "operates in a highly regulated industry," the court concluded that the directors "should have understood" the problem and intervened to fix it. Also notably, the "corporate trauma" alleged was a stock drop upon the announcement of bad news for the company's financial expectations—the typical stuff of federal securities claims—rather than corporate liability for public-facing corporate crimes or torts that are more often the basis of duty-to-monitor claims.

Blue Bell and *Clovis* serve as important reminders that the identification, management and proper monitoring of key corporate risks is a core governance task for boards today. Indeed, one-size-fits-all approaches to risks facing the company need to be replaced with tailored approaches in which more intensive risk management and board-level reporting protocols are applied to risks that may fairly be viewed as "mission critical" on a company-specific and industry-specific basis, including but not limited to heavily regulated industries, products and services.

SEC Risk Disclosure Rules and Stock Exchange Rules

The Securities and Exchange Commission (SEC) requires companies to disclose in their annual reports "factors that make an investment in a registrant's securities speculative or risky." While the SEC has emphasized that risk factor disclosures should be concise, there is a growing concern that the SEC's increasing disclosure requirements have made companies feel compelled to over-disclose and to provide "boilerplate" risk factors that have limited the utility of the disclosures. In this regard, the SEC proposed eliminating the risk factor examples provided in Item 503(c) of Regulation S-K (now Item 105), because "the inclusion of these examples could suggest that a registrant must address each one of its risk factor disclosures, regardless of the significance to its business." In August of 2019, the SEC proposed for public comment a set of amendments that effect this change by, among other things, refining the principles-based approach of Item 105 by changing the disclosure standard from the "most significant" risk factors to "material" risk factors, and requiring a new summary section for risk factor disclosures where the full risk factor disclosure exceeds 15 pages. These proposed amendments are designed to make it easier for investors to identify the most important risk disclosures.

The SEC also 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.

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.

FCPA and Anti-Corruption

Under the Department of Justice's (DOJ) FCPA Corporate Enforcement Policy, when a company voluntarily self-discloses misconduct, fully cooperates, timely and appropriately remediates and agrees to disgorge any ill-gotten profits, there is a presumption that the DOJ will decline to prosecute the company. That presumption will be overcome only if there are aggravating circumstances related to the nature and seriousness of the offense, such as where the company was a repeat offender or where the misconduct was pervasive, involved executive management or resulted in significant corporate profits. In March 2018, the DOJ expanded the scope and applicability of the policy. The DOJ announced that, going forward, the FCPA Corporate Enforcement Policy would serve as "nonbinding guidance" in *all*—not just FCPA-related—Criminal Division corporate fraud investigations. During the summer and fall of 2018, the DOJ further clarified that the benefits of the FCPA Corporate Enforcement Policy are available to companies that promptly self-report corporate wrongdoing discovered in the context of an acquisition or a merger, whether the conduct is FCPA-related or not.

Meanwhile, commitment to anti-corruption enforcement is on the rise across the globe. The DOJ and SEC have pledged continued vigorous enforcement of the FCPA, and have brought significant enforcement actions against both individuals and corporations. In countries from Europe to South America to Asia, new anti-corruption laws are taking effect, and enforcement actions are being pursued. Moreover, corruption investigations have become increasingly international in nature, with significant FCPA cases involving coordinated international resolutions, where multiple countries imposed penalties and shared penalty proceeds.

Dodd-Frank

The Dodd-Frank Act created new federally mandated risk management procedures principally for financial institutions. Dodd-Frank requires bank holding companies with total assets of $10 billion or more, and certain other non-bank financial companies, to have a separate risk committee which includes at least one risk management expert with experience managing risk 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. Examples include reports by the National Association of Corporate Directors (NACD) Blue Ribbon Commission on Risk Governance, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the Conference Board.

In 2017, COSO released the final version of its updated internationally recognized enterprise risk management framework, which it originally released in 2004. As revised, the COSO approach presents five interrelated components of risk management: risk governance and culture (the tone of the organization); setting objectives; execution risk (the assessment of risks that may impact achievement of strategy and business objectives); risk information, communication and reporting; and monitoring enterprise risk management performance. Additional changes adopted in the revised framework are a simplified definition of enterprise risk management designed to be accessible to personnel not directly involved in risk management roles; a clear examination of the role of culture; an elevated discussion of strategy; a renewed emphasis between risk and value; an enhanced alignment between performance and enterprise risk management; a more explicit linking of enterprise risk management to decision-making; an enhanced focus on the integration of enterprise risk management; a refined explanation of the concept of risk appetite and acceptable variation in performance (*i.e.*, risk tolerance); and a clear delineation between enterprise risk management and internal controls. By understanding and emphasizing the relationship between critical assumptions underlying business strategy and risk management, the board can strengthen its risk oversight role.

Recognizing that calls for 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 is intended to bring ESG risks into clearer focus as companies around the world confront an "evolving landscape of ESG-related risks"—from extreme weather events to product safety recalls—that can "impact [the companies'] profitability, success and even survival." The guidance offers an enterprise risk management approach that runs from governance to risk identification and assessment through to communication and reporting.

In June 2019, the Institute of Internal Auditors (IIA) released an exposure draft with proposals on how to improve its 20-year-old "Three Lines of Defense" model in risk management. Under the current version of the model, (1) management control is the first line of defense, (2) the various risk control and compliance oversight functions established by management are the second line of defense and (3) independent assurance is the third line of defense.

Over the last several months, the IIA has evaluated the feedback of over 2,000 commenters, including several that discuss expanded expectations for boards of directors, and has announced an anticipated release of its updated position paper in 2020. It remains to be seen what final changes are implemented, but an enhanced role for the board in "ensur[ing] that roles and responsibilities are clearly understood by all functions, supported by regular interaction and communication" is clear.

Both COSO and IIA, 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 be proactively integrated into strategic planning and prioritized as part of board and CEO-level governance and oversight.

III. STRONG INVESTOR FOCUS ON RISK MANAGEMENT CONTINUES

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 a 2018 NACD 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." As further discussed below, this investor focus has become especially acute in the area of ESG and sustainability-related risks.

Major institutional investors such as BlackRock, State Street and Vanguard believe that sound risk oversight practices are key to enhancing long-term, sustainable value creation. BlackRock has indicated that it expects boards to have "demonstrable fluency" in areas of key risks that affect the company's business and management's approach to addressing and mitigating those risks, and that it will assess this through corporate disclosures and, if necessary, direct engagement with independent directors. BlackRock has cautioned that it "may signal concern through its vote, most likely by voting against the re-election of certain directors" that it deems most responsible for board process and risk oversight. State Street has emphasized that "good corporate governance necessitates the existence of effective internal controls and risk management systems, which should be governed by the board" and will actively seek direct dialogue with the board and management of companies to "protect longer-term shareholder value from excessive risk due to poor governance and sustainability practices."

Vanguard has become particularly active in engaging with boards on the topic of risk oversight, viewing directors as the "shareholders' eyes and ears on risk" and relying "on a strong board to oversee the strategy for realizing opportunities and mitigating risks." Vanguard reiterated this sentiment in its 2019 Investment Stewardship Annual Report, noting that through its "thousands of conversations with company boards and leaders," Vanguard "aim[s] to assess how deeply boards understand their companies' strategies and the associated risks—both known ones and those they may confront in the future." Vanguard has also now adopted formal "oversight failure" voting guidelines in which Vanguard funds will consider voting "against directors who have failed to address material risks and business practices under their purview based on

committee responsibilities" and "when a specific risk does not fall under a specific committee, a [Vanguard] fund will vote against the lead independent director and chair."

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 the 2020 update to its Global Proxy Voting Guidelines, ISS added risk oversight failures to the set of factors that will increase the likelihood of the proxy advisory firm supporting an independent chair proposal, specifically "evidence that the board has failed to oversee and address material risks facing the company" or evidence of "a material governance failure." ISS's Governance QualityScore—a data driven scoring and screening tool that ISS is encouraging institutional investors to use to monitor portfolio company governance—also focuses heavily on boards' audit and risk oversight. ISS has noted that failures of risk oversight include, but are not limited to, bribery, large or serial fines or sanctions from regulatory bodies, significant adverse legal judgments or settlements.

Given the increased focus by institutional investors on ESG risks, Glass Lewis made noteworthy revisions to its proxy voting guidelines to reflect its approach to evaluating board oversight of such risks. For large cap companies and in instances where Glass Lewis identifies material oversight issues, Glass Lewis will review a company's overall governance practices and identify which directors or board-level committees have been charged with oversight of environmental and/or social issues and also note instances where such oversight has not been clearly defined in the company's governance documents. Where Glass Lewis believes that a company has not properly managed or mitigated environmental or social risks or that such mismanagement has threatened shareholder value, Glass Lewis may consider recommending that shareholders vote against those directors who are responsible for oversight of environmental and social risks. In the absence of explicit board oversight of environmental and social issues, Glass Lewis may recommend that shareholders vote against members of the audit committee.

The following are just a few examples of adverse voting recommendations made by ISS and Glass Lewis in response to perceived failures of risk oversight:

- In the 2017 proxy season, ISS recommended that shareholders vote against 12 out of 15 Wells Fargo directors, including the company's independent chairman, on the theory that the board committees "tasked with risk oversight failed over a number of years to provide a timely and sufficient risk oversight process that should have mitigated the harmful impact of the unsound retail banking sales practices that occurred" during that time period.

- In the 2018 proxy season, ISS called for Equifax investors to vote against the re-election of five directors in light of the company's massive data security breach. ISS stressed that the five directors, each of whom served on the company's technology committee at the time of the breach, "had clear lines of responsibility for

risk management related to technology security," yet the breach and Equifax's subsequent failure to quickly notify the public "suggest a failure to adequately oversee some of the most significant risks facing the company."

- In the 2019 proxy season, Glass Lewis recommended the removal of Boeing's audit committee head, citing fatal crashes of the company's 737 MAX plane as evidence of a potential lapse in the board's oversight of risk management. In a note to the board, Glass Lewis wrote that it believed "the audit committee should have taken a more proactive role in identifying the risks associated with the 737 MAX 8 aircraft." Glass Lewis further wrote that it believed "shareholders would be best served with rotation at the board level of the Company's risk management function." ISS similarly recommended that shareholders support a proposal to split the board's chairman and chief executive roles—"the most robust form of independent board oversight"—in light of the potential breakdown in risk management.

IV. RECOMMENDATIONS FOR IMPROVING RISK OVERSIGHT

As an oversight matter, the board should seek to promote an effective, on-going risk dialogue with management, design the right relationships between the board and its standing committees as to risk oversight and ensure appropriate resources support risk management systems. 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 semi-annual basis; and (6) document the existence of risk management protocols and appropriate board-level engagement on risk matters.

Specific types of actions that the board and appropriate board committees may consider as part of their risk management oversight include the following:

- 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 and action plans to be employed if a given risk materializes;

- review with committees and management the board's expectations as to each group's respective responsibilities for risk oversight and management of specific risks to ensure a shared understanding as to accountabilities and roles; establish a clear framework for holding management accountable for building and maintaining an effective risk appetite framework and providing the board with regular, periodic reports on the company's residual risk status;

- review with management the company's risk appetite and risk tolerance and assess whether the company's strategy is consistent with the agreed-upon risk appetite and tolerance for the company;

- review with management the ways in which risk is measured on an aggregate, company-wide basis, the setting of aggregate and individual risk limits (quantitative and qualitative, as appropriate), the policies and procedures in place to hedge against or mitigate risks and the actions to be taken if risk limits are exceeded;

- review with management the assumptions and analysis underpinning the determination of the company's principal risks and whether adequate procedures are in place to ensure that new or materially changed risks are properly and promptly identified, understood and accounted for in the actions of the company;

- review the company's executive compensation structure and incentive programs to ensure they are appropriate in light of the company's articulated risk appetite and risk culture and to ensure they are creating proper incentives in light of the risks the company faces and encouraging, rewarding and reinforcing desired corporate behavior and compliance;

- review the risk policies and procedures adopted by management, including procedures for reporting matters to the board and appropriate committees and providing updates, to assess whether they are appropriate and comprehensive;

- review management's implementation of its risk policies and procedures, to assess whether they are being followed and are effective;

- review with management the quality, type and format of risk-related information provided to directors;

- review the steps taken by management to ensure adequate independence of the risk management function and the processes for resolution and escalation of differences that might arise between risk management and business functions;

- review with management the design of the company's risk management functions, as well as the qualifications and backgrounds of senior risk officers and the personnel policies applicable to risk management, to assess whether they are appropriate given the company's size and scope of operations;

- 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 non-compliance in and outside of the organization; accountability mechanisms designed to ensure that employees at all levels understand the company's approach to risk as well as its risk-related goals; an environment that fosters open communication and that encourages a critical attitude towards decision-making;

and an incentive system that encourages, rewards and reinforces the company's desired risk management behavior;

- review with management the means by which the company's risk management strategy is communicated to all appropriate groups within the company so that it is properly integrated into the company's enterprise-wide business strategy;

- review internal systems of formal and informal communication across divisions and control functions to encourage the prompt and coherent flow of risk-related information within and across business units and, as needed, the prompt escalation of information to senior management (and to the board or board committees as appropriate); and

- review reports from management, independent auditors, internal auditors, legal counsel, regulators, stock analysts and outside experts as considered appropriate regarding risks the company faces and the company's risk management function, and consider whether, based on each individual director's experience, knowledge and expertise, the board or committee primarily tasked with carrying out the board's risk oversight function is sufficiently equipped to oversee all facets of the company's risk profile—including specialized areas such as cybersecurity and the risks that are most critical and relevant to the company and its industry—and determine whether subject-specific risk education is advisable for such directors.

The board should formally undertake an annual review of the company's risk management system, including a review of board- and committee-level risk oversight policies and procedures, a presentation of "best practices" to the extent relevant, tailored to focus on the industry or regulatory arena in which the company operates, and a review of other relevant issues. In the wake of *Blue Bell*, directors should also implement effective procedures to ensure that the board itself monitors key corporate risk factors on an ongoing basis. To this end, it may be appropriate for boards and committees to engage outside consultants to assist them in both the review of the company's risk management systems and also assist them in understanding and analyzing business-specific risks. But because risk, by its very nature, is subject to constant and unexpected change, boards should keep in mind that annual reviews do not replace the need to regularly assess and reassess their own 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 to fruition, management should investigate and report back to the full board or the relevant committees as appropriate.

In addition to considering the foregoing measures, the board may also want to focus on identifying external pressures that can push a company to take excessive risks and consider how best to address those pressures. In particular, companies have come under increasing pressure in recent years from hedge funds and activist shareholders to produce short-term results, often at the expense of longer-term goals. These demands may include steps that would increase the company's risk profile, for example, through increased leverage to repurchase shares or pay out special dividends, spinoffs that leave the resulting companies with smaller capitalizations or underinvestment in areas important to the future competitiveness of the company. While actions

advocated by activists may make sense for a specific company under a specific set of circumstances, the board should focus on the risk impact and be ready to resist pressures to take steps that the board determines are not in the company's or shareholders' best interest, as well as to explain its decisions to its shareholders.

Situating the Risk Oversight Function

While fundamental risks to the company's business strategy are often discussed at the full board level, most 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 policies with respect to risk assessment and risk management. In practice, this delegation to the audit committee may become more of a coordination role, at least insofar as certain kinds of risks will naturally be addressed across other committees as well (*e.g.*, risks arising from compensation structures are frequently considered in the first instance by the compensation committee and matters relating to board and executive succession are often addressed by the nominating and governance committee).

In recent years, the percentage of boards with a separate risk committee has grown, but that percentage remains relatively low. According to a 2019 Deloitte survey, only about 20% of the companies surveyed had a standing risk committee. As discussed earlier in this memo, financial companies covered by 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. Furthermore, different kinds of risks may be best suited to the expertise of different committees—an advantage that may outweigh any benefit from having a single committee specialize in risk oversight. Banks, for instance, often maintain credit or finance committees, while energy companies may have public policy committees largely devoted to environmental and safety issues. It is notable that Boeing, in the wake of two fatal crashes of its 737 MAX airplanes and subsequent regulatory and public scrutiny, announced the creation of a permanent aerospace safety committee on the Board of Directors, a new Product and Services Safety organization that would review all aspects of product safety, and other safety and product-related enhancements to sharpen the company's focus on product and services safety.

Regardless of the delegation of risk oversight to committees, the full board should satisfy itself that the activities of the various committees are properly coordinated and that the company has adequate risk management processes in place. If the company keeps the primary risk oversight function within the audit committee, the audit committee should schedule time for periodic review of risk management outside the context of its role in reviewing financial statements and accounting compliance.

Lines of Communication and Information Flow

The ability of the board or a committee to perform its oversight role is, to a large extent, dependent upon the relationship and the flow of information among the directors, senior management and other senior risk managers in the company. If directors do not believe they are receiving sufficient information, they should be proactive in asking for more. High-quality,

timely and credible information provides the foundation for effective responses and decision-making by the board.

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) charged with risk oversight 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 need the immediate attention of the board outside of the regular reporting procedures. In light of the *Caremark* standards discussed above, the board should feel comfortable that red flags or "yellow flags" are being reported to it so that they may be investigated if appropriate.

Legal Compliance Programs

Senior management should provide the board or 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 will need to be tailored to the specific company's 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 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 the DOJ will assess under the Federal Sentencing Guidelines in the event that corporate personnel do engage in misconduct. Moreover, under the DOJ's updated guidance for white-collar prosecutors, which identifies factors to be considered in evaluating corporate compliance programs, prosecutors may "reward efforts to promote improvement and sustainability" of compliance programs in the form of any prosecution or resolution. Thus, companies with robust compliance programs that continually improve based on lessons learned and data gathered have a real opportunity to benefit.

In keeping with the DOJ's guidance, a compliance program should be designed by persons 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 is not followed will end up hurting rather than helping. 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 that employees understand when and to whom they should report suspected violations and so that 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 facilitating employee education and issuing periodic reminders. If there is a specific area of compliance that is critical to the company's business, the company may consider developing a separate compliance apparatus devoted to that area.

Companies should also assess the extent to which risk management policies and procedures and codes of conduct and ethics are incorporated into the company's strategy and business operations, including promotion and compensation procedures, and supported by appropriate supplementary training programs for employees and regular compliance assessments.

As the *Blue Bell* and *Clovis* cases discussed above and other instances of compliance failures underscore, boards are increasingly coming under scrutiny, fairly or unfairly, when the company fails to meet compliance and legal obligations. Accordingly, it is important that companies develop and cultivate high-performing and well-integrated legal and compliance programs that are supported by executive management and the board.

A Lesson from Wells Fargo on Risk Oversight

In 2018, the Federal Reserve instituted an enforcement action against Wells Fargo, which, among other things, contained several statements regarding the Federal Reserve's view on the responsibility that boards of directors have with respect to risk management. The Federal Reserve:

- characterized compliance breakdowns as failures of governance and board oversight;
- noted replacement of board members;
- censured directors with publicly released letters of reprimand even after they had left the board for "lack of inquiry and lack of demand for additional information";
- expressed the view that a board's composition, governance structure and practices should support the company's business strategy and be aligned with risk tolerances;
- expressed the view that business growth strategies be supported by a system for managing all key risks, including those arising from performance pressure and compensation incentive systems and the potential that business goals could motivate compliance violations and improper practices;
- expressed the view that "management assurances" of enhanced monitoring and handling of known misconduct be backed up by "detailed and concrete plans" reported to the board; and
- referred to the company's published corporate governance guidelines as containing duties and responsibilities that were not fulfilled.

In January 2019, Wells Fargo reported that the Federal Reserve's asset cap on the bank—which prevents the bank from growing past $1.95 trillion in assets—would last longer than expected. Wells Fargo had previously reported that it expected the Federal Reserve to lift the cap in the first part of 2019, but according to the January disclosure, the cap will continue to be imposed through the end of the year.

Since the Federal Reserve's enforcement action and the California fiduciary duty ruling in 2017, other developments at Wells Fargo include the appointment and recruitment of a new permanent CEO from outside of Wells Fargo, new hires in the general counsel, chief risk officer, head of human resources, head of technology and chief auditor positions and further changes in the composition of the board of directors and its committees.

While the Federal Reserve's regulatory authority over banks enables it to impose greater responsibility for risk management on bank directors than is imposed by state corporation law on directors of non-bank corporations, it is important to note the Federal Reserve's views in the Wells Fargo matter as they will undoubtedly be cited and argued in future non-bank cases. Boards should reflect on the expectations with respect to assuring that appropriate risk management systems are in place. This includes setting high expectations for general counsel and compliance departments, as well as following up with robust and prompt inquiry when evidence emerges of material compliance breakdowns.

V. SPECIAL CONSIDERATIONS REGARDING ESG AND SUSTAINABILITY-RELATED RISKS

ESG risks represent a specific subset of general risks that a company should manage, where relevant, by identifying and mitigating company-specific risks, such as environmental liabilities, labor standards, consumer and product safety and leadership succession, and contingency planning for macro-level risks, including by identifying supply chain and energy alternatives and developing backup recovery plans for climate change and other natural disaster scenarios. While boards have been overseeing management of such material risks for as long as they have existed, increasing scrutiny of ESG issues by the public and some of the largest institutional investors in the world now calls for special attention to be paid to ensuring that the board is satisfied with how ESG-related risks are being evaluated, disclosed and managed.

Investor Focus on ESG Risks

Major institutional investors increasingly view ESG issues as having the potential to significantly affect a company's long-term financial value. As stated in a 2018 letter by Chairman and CEO of BlackRock, Laurence D. Fink, "In the current environment . . . stakeholders are demanding that companies exercise leadership on a broader range of issues. And they are right to: a company's ability to manage environmental, social, and governance matters demonstrates the leadership and good governance that is so essential to sustainable growth[.]" BlackRock has further remarked that just as it expects companies to understand the macroeconomic and industry trends in which they operate, it also believes that a company's awareness of ESG-related trends helps drive long-term performance and mitigate risk. In 2019, Fink went even further, imploring companies to heed the "inextricable link" between "purpose and profit." Fink observed that "society is increasingly looking to companies, both public and private, to address pressing social and economic issues," ranging from "protecting the environment to retirement to gender and racial inequality." It is for this reason that BlackRock will engage with a company if it has been identified as lagging its peers on ESG matters that may materially impact long-term economic value.

State Street has been an increasingly vocal and thoughtful advocate of ESG risk oversight, and in 2017 and 2018 issued a series of frameworks and reports for directors regarding

such matters, especially as to integrating sustainability and ESG-related risk matters into corporate strategy. In addition, State Street recently indicated that it will continue to focus on climate risk and reporting as one of its "core, multi-year campaigns." State Street observed that, as of 2018, most companies were beginning to respond to climate-related disclosure recommendations. Although this "is a positive step," State Street sees more work ahead to fully implement climate-related recommendations and effectively manage this risk.

In a nod towards expecting heightened transparency from public companies regarding sustainability-related matters, Vanguard in 2019 emphasized that: "Investors benefit when the market has better visibility into significant risks to the long-term sustainability of a company's business. The evaluation and disclosure of significant risks to a business arising from various potential factors, including environmental and social concerns, result in a more accurate valuation of the company. Accurate valuation over time is critical to ensuring that our fund shareholders are appropriately compensated for the investment risks they assume."

Investors surveyed as part of Ernst & Young's April 2019 Board Matters report echoed State Street's sentiment: 49% of investors said a top board focus for 2019 should be business-related environmental and social factors, and 38% of investors overall are specifically focused on climate change. PwC's 2018 Annual Corporate Directors Survey warned, however, that "directors don't seem to be on the same page," with 39% of directors reporting that climate change "should not be taken into account at all when forming company strategy." Investors are therefore likely to continue pressing this issue.

Recommendations for Improving ESG Risk Oversight

As the public conversation on the role of companies in addressing environmental and social issues continues to evolve, boards should consider how their risk oversight role specifically applies to ESG-related risk. In large part, the board's function in overseeing management of ESG-related risks, such as supply chain disruptions, energy sources and alternatives, labor practices and environmental impacts, involves issue-specific application of the risk oversight practices discussed in this memorandum. However, due to the fact that the public and investors have increasingly begun to scrutinize how a company addresses ESG issues, the board should ensure that its risk oversight role is satisfied in regards to ESG risk management.

ESG matters often have important public, investor and stakeholder relations dimensions. The board should work with management to identify ESG issues that are pertinent to the business and its customers and decide what policies and processes are appropriate for assessing, monitoring and managing ESG risks. The board should also be comfortable with the company's approach to external reporting of the company's overall approach, response and progress on ESG issues. It is also increasingly important for directors and management who engage with shareholders to educate themselves and become conversant on the key ESG issues facing the company.

Boards may also wish to consider receiving briefings as appropriate on relevant ESG matters and the company's approach to handling them. Creating more focused board committees or subcommittees, such as a "corporate responsibility and sustainability" committee, that is specifically tasked with oversight of specified ESG matters, or updating existing committee

charters and board-level corporate governance guidelines to address the board's approach to such topics, may also be considered. Of course, the board should ensure that any committee tasked with ESG risk oversight properly coordinates with any other committees tasked with other types of risk oversight (*i.e.*, the audit committee) and that the board as a whole is satisfied as to the company's approach on these matters.

VI. SPECIAL CONSIDERATIONS REGARDING CYBERSECURITY AND DATA-PRIVACY RISK

The ever-increasing dependence on technological advances that characterizes all aspects of business and modern life has been accompanied by a rapidly growing threat of cyber-crime, the cost of which, according to a 2017 report by Herjavec Group, is expected to grow to more than $6 trillion annually by 2021. As recent examples have highlighted, network security breaches, damage to IT infrastructure and theft of personal data, trade secrets and commercially sensitive information are omnipresent risks that pose a significant financial and reputational threat to companies of all kinds. With computing devices increasingly embedded in everyday items and connected to the "Internet of Things," virtually all company functions across all industries are exposed to cybersecurity risk.

In light of the growing number of successful cyber-attacks on even the most technologically sophisticated entities, lawmakers and regulators in the United States and around the world have increased their attention to cybersecurity risk. In the United States, regulatory and enforcement activity relating to cybersecurity has continued to ramp up at the state level. Internationally, the EU's General Data Protection Regulation (GDPR) has significantly increased data handling requirements for companies with even a minimal European nexus. Companies are thus facing a two-front storm, with regulatory risks compounding the security threat.

Legal and Regulatory Focus on Cybersecurity and Data Privacy

The GDPR, which took effect in 2018, sweeps more broadly than some non-EU-based companies may realize. The GDPR imposes stringent requirements on both data collection and data processing, including increased data security mandates, enhanced obligations to obtain data owner consent and strict breach notification requirements. Importantly, the GDPR is extraterritorial in its reach, and carries severe penalties for noncompliance—up to 4% of worldwide revenue. In 2019, data protection authorities in France and the United Kingdom have announced hefty fines for GDPR violations, penalizing companies for inadequate data security, insufficient cyber-related M&A due diligence, and deficiencies in the processing of personal data. European data protection authorities can be expected to pursue additional major enforcement actions as their GDPR enforcement programs gain traction and mature.

Just a month after the GDPR took effect, California enacted the most expansive data privacy law in the United States to date. The California Consumer Privacy Act (CCPA), which is scheduled to take effect on January 1, 2020, will impose wide-ranging data obligations on companies doing business in California, requiring increased data use transparency and the observance of novel consumer data rights. The primary engine for CCPA enforcement will be the California Attorney General, who can impose fines for violations, but the statute also provides consumers with a private right of action to pursue remedies for harms caused by data breaches. Meanwhile, the New York State Department of Financial Services (DFS) has implemented de-

tailed and prescriptive regulations of its own, requiring covered institutions—entities authorized under New York State banking, insurance or financial services laws—to meet strict minimum cybersecurity standards. The revised regulations require, among other things, that covered institutions have in place a cybersecurity program designed to protect consumers' private data, approved by boards of directors or senior corporate officers and accompanied by annual compliance certifications, the first of which was required to be filed in February of 2018. With a dozen states and Congress considering bills modeled on the CCPA or the GDPR, companies will likely need to navigate an increasingly complex terrain marked by varying state laws and regulations.

The Federal Trade Commission (FTC) has also stepped up its regulatory attention to data privacy and cybersecurity. In July 2019, the FTC imposed a $5 billion penalty and extracted extensive remedial requirements through a controversial settlement with Facebook. The resolution includes not only the largest data privacy penalty in the agency's history, but a broad remedial order that requires a restructuring of Facebook's privacy operations. But aspects of the resolution prompted backlash from dissenting FTC Commissioners and critics in Congress for failing to hold individual executives accountable and to impose more extensive limits on Facebook's collection and use of consumer data. The FTC action—and the controversy it has generated—will likely prompt close scrutiny from Congress, as it weighs whether to increase the agency's reach and authority as part of a possible overhaul of federal data privacy law.

Meanwhile, during the same month, Equifax Inc. announced that it had agreed to pay between $575 and $700 million in a settlement with the FTC, the Consumer Financial Protection Bureau and 50 U.S. states and territories to resolve allegations that the company's failure to take reasonable steps to secure its network led to a data breach affecting approximately 147 million people. The FTC alleged that Equifax failed to patch its network after being alerted in March 2017 to a critical security vulnerability affecting its ACIS database, which handles inquiries from consumers about their personal credit data. In its press release announcing the settlement, the FTC stressed that "companies that profit from personal information have an extra responsibility to protect and secure that data."

For its part, the SEC has turned its attention to market disclosure, breach notification and internal controls. Since 2011, when the SEC's Division of Corporation Finance issued interpretive guidance regarding cybersecurity disclosures, public companies have been required 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." In 2018, the SEC issued new guidance to clarify its expectations as to such disclosures. The majority of the 2018 guidance focuses on "reinforcing and expanding upon" the 2011 guidance, advising public companies to evaluate the materiality of cyber risks and incidents and make necessary disclosures in a timely fashion, while warning that the SEC is watching closely. However, the 2018 guidance delves into some new areas—particularly board oversight, disclosure controls and procedures, insider trading and selective disclosures. As it regards risk oversight, the 2018 guidance advises that public companies should disclose the role of boards in cyber risk management, at least where cyber risks are material to a company's business. Therefore, while most boards are likely already engaged in some form of cyber risk oversight, the call by the SEC for more public disclosure may prompt consideration of whether to deepen or sharpen that engagement.

On the enforcement side, the SEC has adopted a more aggressive approach, engaging in high-profile enforcement actions following its investigations of major data breaches at Yahoo! and Equifax and data privacy practices at Facebook. In 2018, the SEC announced that Altaba, the entity formerly known as Yahoo!, had agreed to pay a $35 million penalty to settle charges that it misled investors by waiting two years to disclose a data breach in which hackers stole the personal information of more than 500 million Yahoo! users. In its press release announcing the settlement, the SEC explained, "We do not second-guess good faith exercises of judgment about cyber-incident disclosure. But we have also cautioned that a company's response to such an event could be so lacking that an enforcement action would be warranted. This is clearly such a case." In July 2019, the SEC announced a $100 million penalty against Facebook for making misleading public disclosures by presenting the risk of misuse of user data as hypothetical, even though numerous employees within the company knew that such misuse had, in fact, occurred. The SEC further found that Facebook did not maintain disclosure controls or procedures to ensure the accuracy of material cyber- and privacy-related risk disclosures, as required of public companies. While the Yahoo! and Facebook cases should not be read as requiring public disclosure of every data breach or privacy violation, the SEC's actions do highlight the need for companies to maintain effective controls and procedures to ensure that internal reports of cyber or privacy incidents, or the risk of such incidents, are properly and timely assessed for potential disclosure.

In 2018, the SEC warned that "directors, officers, and other corporate insiders must not trade a public company's securities while in possession of material nonpublic information, which may include knowledge regarding a significant cybersecurity incident experienced by the company." Later in the year, the DOJ and SEC filed criminal and civil charges against two former Equifax employees—a chief information officer and a software engineer—for insider trading in advance of the company's 2017 disclosure of its breach, with both employees ultimately pleading guilty to the charges against them. In light of the government's enhanced focus on the intersection between cybersecurity and insider trading, companies would be wise to examine their insider trading policies to ensure they operate effectively in the wake of cyber incidents, including by ensuring that consideration is given in any specific situation whether to restrict trading by insiders before public disclosure.

Recommendations for Improving Cyber Risk Oversight

Companies should implement comprehensive cybersecurity risk mitigation programs, deploying defensive technologies without losing focus on core security procedures like patch installation and employee training, executing data and system testing procedures, implementing effective and regularly exercised cyber incident response plans, and ensuring that the board is engaged in cyber risk oversight.

As cybersecurity risk continues to rise in prominence, so too has the number of companies that have begun to specifically address cybersecurity and cyber risk within their internal audit function. A 2019 Internal Audit Capabilities and Needs Survey, conducted by Protiviti, revealed that, of the top 10 audit plan priorities for 2019, cybersecurity risk is the second biggest priority for internal audit groups. Directors should assure themselves that their company's internal audit function includes personnel with the necessary technical expertise and sufficient time and resources to devote to cybersecurity risk. Further, the internal audit team should

understand and periodically test the company's risk mitigation strategy, and provide timely reports on cybersecurity risk to the board's audit committee. An October 2018 report of an investigation by the SEC of cyber frauds committed against a number of companies raises the possibility that a failure to have controls adequate to prevent such frauds could constitute a violation of the securities law requirement to maintain effective internal accounting controls.

In satisfying their risk oversight function with respect to cybersecurity, boards should evaluate their company's preparedness for a possible cybersecurity breach, as well as the company's action plan in the event that a cybersecurity breach occurs. With respect to preparation, boards should review management's risk assessment and mitigation strategies in the key areas identified below and consider whether the company has addressed the following matters, several of which are also discussed in The Conference Board's "A Strategic Cyber-Roadmap for the Board" released in 2016:

- identification of the company's "Crown Jewels"—*i.e.*, the company's mission-critical data and systems;

- application of the protocol outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, a critical benchmarking tool used not only by businesses across the globe, but by key regulators like the SEC and the FTC;

- institution of an actionable cyber incident response plan that, among other things, identifies critical personnel and designates responsibilities; includes procedures for containment, mitigation and continuity of operations; and identifies necessary notifications to be issued as part of a preexisting notification plan;

- development and implementation of effective response technology and services (*e.g.*, off-site data back-up mechanisms, intrusion detection technology and data loss prevention technology);

- establishment of prior authorizations to permit network monitoring;

- access to legal counsel and technical advisers who are conversant with technology systems and cyber incident management to reduce response time; and

- establishment of relationships with cyber information-sharing organizations and engagement with law enforcement before a cybersecurity incident occurs.

The Conference Board Governance Center's 2017 report, "The State of Digital and Social Media Risk Management," also contains useful recommendations for managing the growing number of risks companies face from digital and social media. The report warns that despite the increasingly digital business landscape, companies continue to focus their risk management efforts on "entrenched issues," like virus protection, but have not developed the capacity to address the more novel digital risks that result from third-party, public and "consumerized" IT infrastructure, *i.e.*, social media. Among other useful recommendations, the report urges

boards to review their IT policies and procedures to ensure that new risks, like brand fraud, bots and breaches, are adequately managed.

VII. CONCLUSION

Anticipating Future Risks

The company's risk management structure should include an ongoing effort to assess and analyze the most likely and most significant areas of future risk for the company, including how the contours and interrelationships of existing risks may change and how the company's processes for anticipating future risks are developed. This includes understanding risks inherent in the company's strategic plans, risks arising from the competitive landscape and the potential for technology and other developments to impact the company's profitability and prospects for sustainable, long-term value creation. Anticipating future risks is a key element of avoiding or mitigating those risks before they escalate into crises. In reviewing risk management, the board or relevant committees should ask the company's executives to discuss the most likely sources of material future risks and how the company is addressing any significant potential vulnerability. Indeed, as stressed in the 2018 NACD Blue Ribbon Commission report referenced above:

> *In an operating environment frequently characterized by the acronym VUCA (volatility, uncertainty, complexity, and ambiguity), boards need to help their organizations do a better job of assessing disruptive risks—those risks that, whether internally- or externally-driven, could have a significant economic, operational, and/or reputational impact—and to help them be better prepared to respond when they occur. We believe this task is not an optional undertaking for directors: it is a critical imperative for the boards of for-profit as well as nonprofit organizations, and for both private and public companies.*

The Road Ahead

Directors face an evolving risk and governance landscape, and boards are now recognized as having an affirmative obligation to use their business judgment in identifying material business and liability risks and working with management in articulating the strategy and the time horizon for mitigating them. The law is clear that properly informed directors are empowered to act to protect the corporate reputation; to understand and have the company take steps to mitigate mission-critical and other material risks; to pursue disclosure and engagement efforts designed to inform investors about global social and environmental developments that threaten long-term corporate health; to safeguard long-term global supply chain relationships; and to strengthen the ability to recruit and incentivize a skilled and motivated workforce. Taken together, directors' duties not only permit boards to address the full range of risks that threaten the corporation's ability to deliver sustainable growth, but indeed require boards to address the most acute among them.

INDEX