BAILEY | CAVALIERI

DAN A. BAILEY
E dbailey@baileycav.com
D 614.229.3213

PROPOSED SEC DISCLOSURE RULES
(Climate Change; Cybersecurity)

May 2022

Although the generic disclosure requirements under the Securities Exchange Act of 1934, when coupled with decades of court decisions interpreting those requirements, provide a detailed framework for disclosure of virtually any type of material information, the SEC in recent years has issued a series of rules which explain in much greater detail the disclosure requirements applicable to specific topics. These rules are often criticized as an attempt by the SEC to legislate behavior regarding politically sensitive topics. Two prominent examples are proposed rules issued by the SEC in 2022 regarding disclosure of cybersecurity risks and climate change issues. Each are summarized below.

1. Climate Change Disclosure Rules.

On March 21, 2022, the SEC issued proposed new rules requiring all registered public companies to disclose a wide range of information related to climate change and greenhouse gas emissions information and risks. The sweeping and highly controversial rules have been described as the most extensive, comprehensive and complicated disclosure initiative in decades.

The proposed rules would, for the first time, require the disclosure to investors of climate risk information, unlike prior practice pursuant to which companies largely provided that information on a voluntary and inconsistent basis with the benefit of non-binding SEC "guidance." The detailed and complex requirements, set forth in the proposal's more than 500 pages, are intended by the SEC "to enhance and standardize climate-related disclosures to address…investor needs." By addressing climate change issues through disclosures to shareholders, the SEC is creating personal accountability for directors and officers who fail to comply with the new requirements. Not only will the SEC be a direct enforcer of the new requirements through proceedings against both the company and its directors and officers, but shareholders (and plaintiff lawyers) will undoubtedly use the new rules as a basis for securities class action lawsuits against directors and officers and their companies. Plus, the rules could increase investor scrutiny over energy project development and investment decisions, leading to more mismanagement claims against directors and officers.

According to the SEC's fact sheet, the proposed new rules address the following basic areas of information.

- Climate-related risks and their actual or likely material impacts on the registrant's business, strategy and outlook, over the short-, medium- and long-term;

- The registrant's governance of climate change risks and relevant risk management processes;

- The amount and nature of the registrant's greenhouse gas ("GHG") emissions;

- Certain climate-change related financial statement metrics and related disclosures in a note to audited financial statements;

- Information about climate-related targets and goals, and any related transition plan; and

- The impact of climate-related events (severe weather events and other natural conditions).

Unquestionably, the proposed rules, if adopted in their proposed form, will have a profound impact on publicly-held companies, particularly those with a significant GHG footprint. The collection, compilation and evaluation of an enormous amount of climate-related data from multiple parts of the company will require the creation, maintenance and funding of a new level of infrastructure and management oversight even for companies that already have a robust climate disclosure process.

From a board of directors perspective, numerous new responsibilities and challenges will arise. For example, the board will need to consider whether the entire board, the audit committee, a risk committee or a stand-alone committee should be tasked with oversight of climate-related risks, disclosures and related internal controls and procedures. The proposed new rules require disclosure of who has that oversight responsibility and how that oversight will occur. The board and senior management also will need to review the company's internal controls and procedures on climate-related disclosures to assure compliance with the extensive new requirements and consistent climate-related reporting to both the SEC and all other federal and state regulatory agencies such as the EPA and FERC. Close coordination between a company's environmental and financial divisions will be important.

The proposed new rules create particularly harsh requirements on decarbonization plans adopted by various types of companies which have publicly-announced net-zero and other long-term GHG emission reduction targets. The SEC proposal would require those plans and any progress made toward achieving the plan's goal to be very detailed. For example, companies will need to disclose any interim emissions reduction targets, data (updated annually) on how a company is meeting its reduction goals, and information on use of renewable energy certificates or carbon offsets. Lack of sufficient detail could create potential disclosure-related liability risks for directors and officers.

Yet another area of concern for directors and officers is the requirement that companies disclose any internal carbon price they use to calculate their return on investment for potential projects or investments and how that internal carbon price is calculated. Those disclosures will give investors and capital providers unprecedented visibility into a board's and management's decision making and could result in investors proactively scrutinizing and challenging those decisions both in real time and after the fact.

Although it is difficult to predict the specific contours or effects of any ultimately adopted rules, it is clear from this SEC initiative that increased disclosure of and investor scrutiny about a company's climate-related behavior and increased accountability of a company's gatekeepers for that behavior are probably here to stay.

2. Cybersecurity Disclosure Rules.

Also in March 2022, the SEC released its long-awaited proposed rules defining a public company's disclosure obligations regarding cybersecurity matters. The proposed rules, which supplement cybersecurity disclosure guidance issued by the SEC in 2011 and 2018,[1] would for the first time create detailed and mandatory disclosure obligations for all public companies regarding material cybersecurity incidents and each company's governance, risk management and strategy regarding cybersecurity risks. The SEC's stated goal is to enhance and standardize disclosures by public companies in this area.

The proposed rules address two categories of disclosures: (i) cybersecurity incident disclosures, and (ii) cybersecurity risk management and governance disclosures.

Cybersecurity Incident Disclosures. The rules would require public companies to disclose in a Form 8-K filing with the SEC any material cybersecurity incident within four business days after the company determines it has experienced a material cybersecurity incident. The four business day deadline for the disclosure is far shorter than otherwise applicable disclosure obligations. Importantly, the disclosure obligation is triggered by a company determining the cybersecurity incident is material (which is not defined in the rules) rather than when the company discovers the incident. The date of that somewhat subjective determination will likely be unclear in many instances, leading to disputes and uncertainties as to whether the disclosures are timely.

The proposed rules also require companies to provide updated disclosures relating to previously disclosed cybersecurity incidents and to disclose when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate.

A "cybersecurity incident" is defined in the proposed rules as an "unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the

[1] CF Disclosure Guidance: Topic No. 2-_Cybersecurity (Oct.13, 2011); Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 26, 2018); No. 33-10459 (Feb. 21, 2018) [83 FR 8166].

confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."

Cybersecurity Risk Management and Governance Disclosures. The rules would also require public companies to disclose in their annual reports and certain proxy statements risk management and governance information regarding cybersecurity matters. The disclosures must include:

- a description of the company's policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the company considers cybersecurity as part of its business strategy, financial planning, and capital allocation;

- a description of the board's oversight of cybersecurity risk and management's role and expertise in assessing and managing cybersecurity risk and implementing the company's cybersecurity policies, procedures, and strategies; and

- identification of any board member with cybersecurity expertise.

Whether or not eventually adopted, these highly publicized proposed rules should incentivize companies to reassess (i) their existing procedures for timely identifying and responding to cyber incidents (including the clear definition of roles and responsibilities within management and the board), (ii) their existing risk management policies and procedures in this area, and (iii) the need for cybersecurity expertise not only within senior management but also the board.