Published on *The National Law Review* https://natlawreview.com

What Will the SEC's ESG Enforcement Look Like? Cyber Cases Offer Clues

Article By:

Philip J. Bezanson

Claire E. Cahoon

As the SEC has become more vocal in its expectations for environmental, social, and government (ESG) disclosure, serious questions remain about how ESG matters will be investigated and what enforcement measures might look like. Indicators suggest that the SEC will establish formal regulations regarding ESG disclosure, and the SEC has simultaneously suggested that it plans to ramp up enforcement across the board where it already has the authority to do so. But, without clear SEC guidance, companies and the marketplace are left to their own devices to determine how ESG matters might be investigated by the SEC and how aggressive the SEC will be in bringing enforcement actions related to ESG disclosures.

Issuers looking for guidance may want to consider looking at the SEC's recent history of adopting cybersecurity and data privacy disclosure rules and attendant enforcement matters.

Historically, the SEC's expectations surrounding a company's cybersecurity and data privacy disclosures have evolved as cyber threats, consumers, and companies have become more cyber-sophisticated. This fluidity complicates rulemaking.

As a result, while cyber risk has been part of SEC discourse for well over a decade, no formal rules specifically address cyber risk disclosure, and legislation mandating such rules has yet to gain any real traction. Instead, companies rely on SEC guidelines, comment letters, and enforcement actions.

Initially, the guidelines that the SEC released in 2011 encouraged companies to disclose details regarding material cyber risks and to disclose known or threatened "material cyber attack[s]" compromising consumer data.[1] In 2017, the SEC announced the creation of the "Cyber Unit," which resembles the recently announced Climate and ESG Task Force, within the SEC's Enforcement Division. The SEC expanded its 2011 guidelines in 2018 by instructing companies to disclose the probability of future incidents, preventative measures and affiliated costs, potential reputational harm in the event of a cyber attack, and ongoing litigation and regulatory investigations associated with cybersecurity incidents.

Issuers have increased transparency regarding cyber risk in recent years. But without mandatory

rules, disclosure has largely been left to issuers' best efforts to be transparent without revealing information that would give hackers a roadmap to potential weaknesses. There are similar incentives for issuers to try to minimize disclosing ESG risks – including regulatory considerations, the potential for private civil actions, and reputational/marketplace risk.

This incentive structure puts pressure on companies to manage public perception of cyber risk and keep their boards informed while simultaneously maintaining sufficiently high-quality cyber policies and practices to repel cyber attacks. A similar juggling act is likely to arise in the area of ESG, as executives balance public perceptions of ESG with substantive ESG concerns. Failure to balance public perception and substance can put companies at financial, reputational, and legal risk, as businesses that have faced litigation and enforcement regarding cyber disclosure have already experienced.

For example, Altaba Inc., formerly known as Yahoo!, paid a $35 million penalty in 2018 to settle SEC charges alleging that Yahoo! made insufficient disclosures regarding its cyber risk in the wake of a cyber attack affecting over 500 million customer accounts. Specifically, the SEC found that Yahoo! failed to fully disclose the substantive impact and legal implications of a cyber breach. Shareholders and consumers have been largely unsuccessful in suing companies based on failures to disclose potential cyber weaknesses.[2] But such lawsuits aren't slowing down any time soon. Shareholders of Solarwinds, which first disclosed the now-infamous malware attack on an SEC Form 8-k, are pursuing a class action lawsuit alleging that SolarWinds under-disclosed cyber risk vulnerability in the lead-up to the attack.

Despite its increasingly strong stance on the importance of cyber issues, the SEC has taken a lighter approach to first-time cyber disclosure violators. The agency has sent comment letters to over 50 companies since 2012 regarding cybersecurity compliance, prompting companies like Amazon and Google to disclose more information relating to data breaches, cyber vulnerabilities, and preventative measures.

While the SEC's similarly strong rhetoric surrounding ESG may suggest aggressive enforcement, the SEC's approach to cyber demonstrates that companies may want to think of ESG disclosure in the same manner recommended for cyber: focus on the substance. Companies can largely avoid risks relating to cyber disclosure by ensuring that its cyber policies and practices are tested and assessed with a critical eye. The SEC has provided guidance on cybersecurity and data privacy best-practices, and Cyber Unit Chief Kristina Littman has advised that willful blindness to cyber-risk is not a smart strategy – companies' first priority should be adherence, and disclosure of adherence, to those best-practices.

Similarly, companies seeking to avoid the risk of improper ESG disclosure should pay close attention to SEC guidance and make sure that substantive ESG policies and practices match the SEC's suggestions, and that those substantive policies and practices are accurately disclosed. The SEC's 2010 guidelines regarding disclosure of climate change risks provide an important starting-point, especially since the SEC says that these guidelines will serve as a baseline for both increased enforcement and future guidance.

As corporations' social reputations play an increasing role in market value, transparent disclosure regarding ESG risk is important to attract, inform, and protect investors. The consequences of improper disclosure are harsh – both under- and over-disclosure can lead to enforcement actions as well as first-party litigation, inflicting significant reputational and financial damage to corporations. But as with cyber, disclosure-related risks surrounding ESG can be avoided by focusing on ESG policy

and practice. Bracewell attorneys are ready and able to help companies navigate the ever-evolving considerations surrounding both ESG and cyber risk disclosure.

---

1. Of course, the SEC has always required disclosure of any “material” risk, which, for some companies, required disclosure of cyber risk long before any SEC guidance existed. But the frequency and cost of cyber attacks continue to rise, making cyber risk “material” to nearly all publicly traded companies.

2. In re Facebook, Inc. Sec. Litig., 477 F. Supp. 3d 980, 1017 (N.D. Cal. 2020); Doyun Kim v. Advanced Micro Devices, Inc., No. 5:18-CV-00321-EJD, 2019 WL 2232545, at *8 (N.D. Cal. May 23, 2019).

National Law Review, Volume XI, Number 99

Source URL:https://natlawreview.com/article/what-will-sec-s-esg-enforcement-look-cyber-cases-offer-clues