Client Alert | US Public Company Advisory / White Collar/Investigations

SEC Enforcement Heats up on Key Public Company Topics: Cyber Disclosure, Director Independence and Regulation FD

November 8, 2024

The U.S. Securities and Exchange Commission's ("SEC") Division of Enforcement has recently brought a spate of enforcement actions relating to key topics for public companies. These include enforcement actions related to cybersecurity incident disclosure, director independence and Regulation Fair Disclosure ("Reg FD") violations, which are described below[1], and actions based on Section 13 and 16 beneficial ownership filings, as discussed in our prior alert.[2]

Cyber Disclosure Enforcement Actions

On October 22, 2024, the SEC announced charges against four companies for making materially misleading disclosures regarding cybersecurity. One company was also charged with disclosure controls and procedures violations.[3] These actions all arose from the SEC's investigation of public companies that were potentially impacted by the compromise of SolarWinds Corp.'s' Orion software.[4] The companies agreed to pay civil penalties ranging from $990,000 to $4 million.

---

1 The SEC's press releases are available at:

- SEC Charges Four Companies with Misleading Cyber Disclosures,
- SEC Charges Independent Director and Ex-CEO of Church & Dwight with Concealing Close Friendship with Company Executive, and
- SEC Charges DraftKings with Selectively Disclosing Nonpublic Information Via CEO's Social Media Accounts.

2 Notably, these were the first SEC enforcement actions on director independence and Reg FD since 2022 and 2021, respectively, and the first SEC enforcement actions regarding cybersecurity disclosures since the SolarWinds Corp. decision in July of this year. The most recent prior SEC action related to director independence was In the Matter of Leaf Group Ltd., in which a "compensation committee interlock" disqualified the director as independent under stock exchange listing standards and also required specific disclosure in Leaf's proxy statement. The most recent action regarding a Reg FD violation was SEC vs. AT&T, et al., where the SEC found that investor relations executives at the company made private, one-on-one calls to analysts disclosing material internal company data and metrics in order to lower consensus revenue expectations for the quarter, and therefore avoid falling short of such expectations, in violation of Reg FD.

3 *See* In the Matter of Unisys Corporation.

4 For more information on the SolarWinds breach and related SEC charges, see our prior alerts, The SEC's Charges Against SolarWinds and its Chief Information Security Officer Provide Important Cybersecurity Lessons for Public Companies and Judge Rejects SEC's Aggressive Approach to Cybersecurity Enforcement.

According to the SEC's orders against each of the four companies[5], the companies had learned that a threat actor likely behind the SolarWinds Orion hack had accessed their systems without authorization, but each negligently minimized these cybersecurity incidents in public disclosures. Specifically, the SEC found that one company's Form 10-K described its risks from cybersecurity events as hypothetical, despite the company knowing that it had experienced two SolarWinds-related intrusions involving the unauthorized transfer of very large amounts of data. The SEC's order also noted that these materially misleading disclosures resulted in part from the company's deficient disclosure controls, stating that the Company's "incident response policies did not reasonably require cybersecurity personnel to report information to [the Company's] disclosure decision makers and contained no criteria for determining which incidents or information should be reported outside the information security organization."[6]

Similarly, the SEC found that another company, a foreign private issuer, knew of the cybersecurity compromise, but in its Form 20-F described cyber intrusions and risks from them in only generic terms and "omitted new and material cybersecurity risks" arising out of the SolarWinds compromise. In another order, the SEC noted that the company stated in its Form 10-Q that the threat actor had accessed a "limited number of [the] Company's email messages," that "there was no current evidence of unauthorized access" and that the company did "not believe that this incident has had or will have a material and adverse impact on our business or operations." In fact, the company knew that at least 145 files in its cloud file sharing environment had been accessed, that there had been a long-term unmonitored presence of the threat actor in the company's systems, the threat actor had accessed the emails of company cybersecurity personnel, and that there was likely involvement of a nation-state as a threat actor. Lastly, the SEC noted that a fourth company filed a Form 8-K that minimized the attack by quantifying certain aspects of the breach but failed to disclose the nature of the code the threat actor targeted and the quantity of encrypted credentials the threat actor accessed.[7]

Overall, the SEC emphasized the importance of not downplaying the extent of a cybersecurity breach and focused on risk factors, noting that "the relevant cybersecurity risk factors were framed hypothetically or generically when the companies knew the warned of risks had already materialized" and that the "federal securities laws prohibit half-truths." SEC Commissioners Peirce and Uyeda issued a joint dissenting statement against these actions, taking the position that the SEC is regulating by enforcement and citing immaterial, undisclosed details to support the charges, details that they do not believe would have altered the "total mix" of information.

It is also notable that the SEC did not charge these companies with violating the internal accounting controls provision, Section 13(b)(2)(B), which was one of the claims that a federal court dismissed in the SolarWinds case. The Court there found that the term "internal accounting controls" refers to a company's "financial accounting," and not cybersecurity controls. Prior to that decision, the SEC often included this charge in their cybersecurity disclosure actions.

Taken together, these actions provide important lessons for public companies about the disclosure of cybersecurity incidents:

- Do not disclose a risk as hypothetical when in fact that risk has already occurred and do not describe specific, known risks in only generic terms.

---

5 The SEC's orders are available at the following:
- In the Matter of Unisys Corporation,
- In the Matter of Avaya Holdings Corp.,
- In the Matter of Check Point Software Technologies Ltd. and
- In the Matter of Mimecast Limited.

6 After investigating its cybersecurity controls, the company "publicly disclosed a material weakness in its disclosure controls and procedures and internal control over financial reporting related to the design and maintenance of effective formal policies and procedures over information being communicated by the IT function and the legal and compliance function to those responsible for governance to allow timely decisions related to both financial reporting and other non-financial reporting."

7 Note that this Form 8-K was filed before the SEC's new cybersecurity disclosure rules were adopted.

- Reassess cyber incident response plans (CIRPs) and related disclosure controls to ensure that material cybersecurity incidents are identified and timely elevated to those responsible for ensuring disclosure of material cybersecurity incidents in SEC filings.
- Evaluate and update existing disclosure to reflect changing circumstances and the company's changed risk profile as a result of any recent cybersecurity incident.
- Describe fully and accurately any cybersecurity incidents that are disclosed; quantifying certain aspects of an incident without disclosing other material information on its scope and impact may be materially misleading. Nonetheless, any disclosures should be balanced against the need for the company to avoid revealing critical information about its cybersecurity controls or risk to protect against future cyberattacks.
- When evaluating materiality, consider, among other factors, the nature of the company's particular business and any confirmed attribution of the incident to nation-state actors or global hacker organizations.

Director Independence

On September 30, 2024, the SEC announced settled charges against a public company director for violating proxy disclosure rules by standing for election as an independent director without informing the board of his close personal friendship with a high-ranking executive, which resulted in a public company's proxy statements containing materially misleading statements regarding his independence.

Specifically, James Craigie, a former CEO and former non-independent corporate director who later served as an independent director, allegedly hid his "close personal relationship" with a company executive from the rest of the board when he completed D&O Questionnaires in which he stated that he did not have a material relationship with the company, including "any other relationship" with the company or its management. According to the SEC's complaint, as a result of his failure to disclose his relationship with a company executive in responses to his D&O questionnaire, the company's proxy statements contained materially misleading statements that inaccurately identified the director as "independent" under both stock exchange listing standards and the company's governance guidelines. When the company ultimately learned of the relationship, it determined that Craigie was not actually independent under these standards based on several factors[8]:

- The director maintained a close friendship with one of the company's executives, which included regular, luxury vacations together with their respective spouses, paid for by the director (totaling over $100,000).[9]
- In addition to not disclosing this relationship to the board during its deliberation over whether he qualified as independent, the director repeatedly requested that the executive keep this relationship a secret, to avoid the appearance of bias.
- When the company began a CEO succession process, the director participated in the process of evaluating internal CEO candidates, including the executive, without disclosing their relationship, and he subsequently revealed the CEO succession discussions to the executive, despite being told to keep the search confidential.
- When the board considered external CEO candidates, the director suggested an individual that he had a relationship with through the executive, again without disclosing this connection to the board, with the specific intention that this could potentially pave the way for the executive to become CEO down the road.

The SEC alleged that, as an "experienced public company executive and board member," the director "knew, or should have known, the criteria that public company boards use to assess a director's independence, as well as the factors that are important to that analysis. This included personal relationships with company executives."

The director also "understood the importance of the D&O Questionnaire for determining director independence," and that the information would be included in the proxy statement. In addition, as a director of other public companies, this director completed other D&O questionnaires, some of which included questions that "further

[8] It is worth noting that while the SEC was investigating Craigie's relationship with the executive, Craigie was instructed not to communicate with other parties, including the executive, and had received a document retention notice from the company. Despite this, Craigie sent a letter to the executive discussing matters relevant to the SEC's investigation and indicated that he should discard the letter after reading it.

[9] Craigie "did not similarly vacation with, nor pay expenses for, other [company] executives."

clarified what facts and circumstances Craigie should have considered when responding to the [company's] questionnaire."

As a result, the SEC found that Craigie was directly liable for the misstatements in the company's proxy statements as to his independent director status because he failed to disclose the relationship in his responses to the D&O Questionnaires, and then permitted his name to be used in connection with the company's proxy solicitation, in violation of Section 14(a) of the Exchange Act and Rule 14a-9.

The case is the latest reminder of the importance of the general independence test. In 2010, the New York Stock Exchange had also focused on this issue, targeting a public company over how a board determined the independence of a director who owned a real estate development with the company's chief executive.[10] In light of this enforcement action, companies are reminded to:

- Consider what types of relationships would impair director independence under the general independence test, including what might be considered a "close personal friendship", and what factors might weigh in favor of a determination that a director lacks independence.
- Ensure your D&O questionnaire asks sufficiently detailed and direct questions to elicit relevant information to assess independence. For example, in the question about the general independence test, consider adding an explanation that personal friendships and other relationships with management should be disclosed and provide examples of the types of relationships that could impair independence. It is also advisable to make clear that the responses to D&O Questionnaires form the basis for disclosures made by the company in its SEC filings.
- Make sure your directors are engaged in the director independence process and disclosing information that would be relevant for an independence assessment and educate your directors and management on the importance of complete and accurate disclosure, and the potential consequences of failures to disclose.

Regulation FD Violations for Disclosing Material Nonpublic Information in Social Media Posts

On September 26, 2024, the SEC charged DraftKings Inc., with violations of Reg FD[11] in connection with the posting of material nonpublic information ("MNPI") to certain social media accounts associated with the company's CEO.[12] According to the SEC, the company's external public relations firm posted MNPI on the CEO's personal X and LinkedIn accounts, including statements about the company's second quarter earnings prior to the company's disclosure of this information to the public. Neither of these accounts was a Reg FD-compliant distribution channel.[13]

Notably, the company's communications team recognized the error and had the posts taken down within half an hour. However, the company did not take any steps to promptly disclose the inadvertently disseminated information to the general public, as required by Reg FD, and instead waited until its previously scheduled earnings release a full week later to disclose the information.

The postings violated the company's social media policy, which prohibited the sharing of such information via social media, and the "quiet period" provisions in its Regulation FD Policy, which prohibited disclosure or discussion of financial

---

10 *See* Wall Street Journal, "Big Board Questions Black & Decker."

11 Reg FD is available here. As a reminder, Reg FD prohibits public companies, or persons acting on their behalf, from selectively disclosing MNPI to certain securities professionals or shareholders who might trade on the basis of such information before it has been made public. Information is considered public for Reg FD purposes if it has been disseminated through a method that is reasonably designed to result in broad, non-exclusionary distribution to the public, such as a broadly disseminated press release or Form 8-K filing. An inadvertent disclosure of MNPI can be cured by making prompt public disclosure of the information (typically within 24 hours).

12 The SEC's press release is available here and its order is available here.

13 Use of company websites or social media accounts as a Reg FD compliant method of distribution is rare. Prior SEC guidance on use of such websites or accounts (2008 interpretive release on Reg FD compliance and 2013 report of investigation of Reg FD compliance) makes clear that public companies who want to use such fora to disseminate information in compliance with Reg FD must first take specific steps to establish that forum as a recognized channel of distribution.

or operational results or guidance, performance during the period prior to an earnings release. The settlement required all company "employees who have responsibilities relating to corporate communications to attend training regarding Regulation FD" and the company's Regulation FD Policy.

Companies are reminded to:

- Ensure that external IR providers are complying with the Company's policies and receiving appropriate oversight from Company management to confirm compliance with Reg FD.
- Ensure that social media accounts of executives are not disclosing any material nonpublic information.
- Cleary identify Reg FD compliant manners of disclosure and communicate these to relevant parties.
- Regularly educate employees and consultants on the requirements of Reg FD and the company's Reg FD policy and provide training on the company's social media and Reg FD policies.
- Quickly cure any inadvertent disclosures within the mandated period under Reg FD (no later than the later of 24 hours or commencement of the next day's trading).

The following White & Case attorneys authored this alert:

Maia Gez
Scott Levi
Paul Pittman
Michelle Rutta
Tami Stark
Danielle Herrick

White & Case Team Members:

A.J. Ericksen: 713-496-9688, aj.ericksen@whitecase.com
Elodie Gal: 212-819-8242, egal@whitecase.com
Maia Gez: 212-819-8217, maia.gez@whitecase.com
David Johansen: 212-819-8509, djohansen@whitecase.com
Scott Levi: 212-819-8329, scott.levi@whitecase.com
Daniel Nussen: 213-620-7796, daniel.nussen@whitecase.com
Kimberly Petillo-Decossard: 212-819-8398, kimberly.petillo-decossard@whitecase.com
F. Paul Pittman: 202-729-2395, paul.pittman@whitecase.com
Jason Rocha: 713-496-9732, jason.rocha@whitecase.com
Jonathan Rochwarger: 212-819-7643, jrochwarger@whitecase.com
Joel Rubinstein: 212-819-7642, joel.rubinstein@whitecase.com
Michelle Rutta: 212-819-7864, mrutta@whitecase.com
Elliott Smith: 212-819-7644, elliott.smith@whitecase.com
Tami Stark: 212-819-2674, tami.stark@whitecase.com
Melinda Anderson: 212-819-7002, melinda.anderson@whitecase.com
Danielle Herrick: 212-819-8232, danielle.herrrick@whitecase.com
Patti Marks: 212-819-7019, pmarks@whitecase.com
Sarah Hernandez: 212-819-8429, sarah.hernandez@whitecase.com

White & Case LLP
1221 Avenue of the Americas,
Floor 49 Reception
New York, NY 10020

T +1 212 819 8200

In this publication, White & Case means the international legal practice comprising White & Case LLP, a New York State registered limited liability partnership, White & Case LLP, a limited liability partnership incorporated under English law and all other affiliated partnerships, companies and entities.

This publication is prepared for the general information of our clients and other interested persons. It is not, and does not attempt to be, comprehensive in nature. Due to the general nature of its content, it should not be regarded as legal advice.

© 2024 White & Case LLP