LEGAL UPDATES

PUBLISHED: AUGUST 12, 2024

# Court Limits an Early SEC Effort at Cybersecurity Enforcement

## Services

Data Privacy & Cybersecurity

Securities & Corporate Governance

## Industry

Financial Services & Capital Markets

## Professionals

**STEVEN R. BARRETT**
**CHATTANOOGA:**
**423.757.5905**
**STEVE.BARRETT@HUSCHBLACKWELL.COM**

**ROBERT J. JOSEPH**
**CHICAGO:**
**312.526.1536**
**ROBERT.JOSEPH@HUSCHBLACKWELL.COM**

**ANDREW SPECTOR**
**BOSTON:**
**617.598.6700**
**ANDREW.SPECTOR@HUSCHBLACKWELL.COM**

On July 18, 2024, Judge Paul A. Engelmeyer of the U.S. District Court for the Southern District of New York issued a 107-page opinion dismissing most of the Securities and Exchange Commission's (SEC) case against SolarWinds Corporation and its chief information security officer (CISO).

### Background

SolarWinds is a publicly traded company that designs and sells business IT monitoring and management software. Beginning in 2019 and continuing through November 2020, threat actors (believed to be state-sponsored actors working for the Russian Foreign Intelligence Service) exploited the corporate VPN of SolarWinds to gain access to its "entire network." These actors harvested customer data and inserted malicious code into the company's software, impacting approximately 18,000 of its customers, including many federal and state government agencies and more than 1,500 publicly traded U.S. companies and other SEC-regulated entities. The malicious code allowed the threat actors to gain a "backdoor into the network environments of SolarWinds' customers[.]" The same threat actors then launched a large scale cyberattack in December 2020 which later became known as the SUNBURST attack.

### The claims

The SEC complaint against SolarWinds and its CISO, filed originally in late 2023 and amended in 2024 in response to pre- and post-SUNBURST disclosures by SolarWinds, alleged that SolarWinds and its CISO (i) made materially false and misleading statements and omissions (on the company website, in blog posts, in press releases, in a Form S-1 registration statement, and in quarterly and annual reports filed with the SEC prior to the cybersecurity incident, and in two Form 8-K current reports filed by the

company in response to the cybersecurity incident), (ii) failed to maintain a system of internal accounting controls sufficient to provide reasonable assurances that access to company assets was permitted only in accordance with management's general or specific authorization, and (ii) failed to maintain a system of disclosure controls and procedures sufficient to ensure that information required to be disclosed is escalated internally to allow for timely disclosure decisions.

**Action by the court**

The court granted the motion by SolarWinds and its CISO to dismiss to all the securities fraud and other claims of violations except the claims relating to a Security Statement published on the company website purporting to describe the company's cybersecurity practices. It is unclear at this time whether the SEC intends to appeal the decision.

*The court dismissed claims related to the company's podcast, press releases, and blog posts.*

The SEC alleged securities fraud violations against SolarWinds and its CISO for public statements made in podcasts, press releases, and blog posts, arguing the statements misled investors about its cybersecurity practices.

The court dismissed these claims as "non-actionable corporate puffery" that were "too general to cause a reasonable investor to rely upon them."

*The court dismissed claims that the company's cybersecurity risk disclosures in the company's Form S-1, annual reports, and quarterly reports were inadequate.*

The SEC alleged material misstatements or omissions by SolarWinds due to its cybersecurity risk disclosure in the company's registration statement on Form S-1 and annual and quarterly reports.

In dismissing these claims, the court noted that spelling out a risk with maximal specificity may backfire in various ways, including by providing information which can be exploited or by misleading investors. The court noted the disclosure of cybersecurity risks was fulsome and that although the disclosures risks were generic, viewed in totality, the disclosures sufficiently alerted the investing public to the company's cybersecurity risks.

*The court dismissed claims that the company's Form 8-K disclosures were insufficient in detail.*

The SEC alleged material misstatements or omissions by SolarWinds in current reports on Form 8-K filed by the company regarding the cybersecurity incident.

The court held that the first Form 8-K disclosed the events surrounding the cybersecurity incident with appropriate gravity and detail and that determining whether disclosure of cybersecurity incidents provided in real time are misleading requires perspective and context.

*The court dismissed claims that the company's cybersecurity deficiencies violated the internal control provisions of Section 13(b)(2)(B) the Securities Exchange Act of 1934.*

The SEC alleged that SolarWinds failed to devise and maintain appropriate internal accounting controls sufficient to provide reasonable assurances that access to assets is permitted only in accordance with management's general or specific authorization. The SEC argued that the company's cybersecurity deficiencies were actionable because the company's source code and databases were its most vital assets and the attacks were possible because of the company's poor access controls.

In dismissing these claims, the court determined that cybersecurity controls were not a part of the company's internal accounting controls, noting that cybersecurity control does not naturally fit within the term "internal accounting controls" because a failure to detect a cybersecurity deficiency cannot reasonably be termed an accounting problem.

*The court dismissed claims that the company's disclosure controls and procedures were ineffective.*

The SEC alleged under Rule 13a-15(a) of the Exchange Act that SolarWinds had ineffective disclosure controls in place due to a misclassification of earlier incidents related to the cybersecurity attacks. Rule 13a-15(a) requires issuers to maintain disclosure controls and procedures sufficient to ensure that information required to be disclosed by an issuer in the reports that it files or submits under the Exchange Act is accumulated and communicated to the issuer's management, including its principal executive and principal financial officers, as appropriate to allow timely decisions regarding required disclosure.

The court determined that SolarWinds did have an effective system of controls in place to facilitate the disclosure of potentially material cybersecurity risks and incidents. The court noted that controls can be reasonably designed even if they are not error free, and errors can occur without systemic deficiencies. The court added that the SEC alleged its claim with the benefit of hindsight and that in securities fraud claims, "second-guessing by hindsight" is disfavored.

*The court allowed claims that the company's Security Statement was materially misleading to proceed.*

The court permitted a narrow category of claims against SolarWinds and its CISO to proceed. The court determined that the SEC's allegations concerning the SolarWinds Security Statement (and its CISO's involvement with the statement) were sufficient to support claims that investors were misled about the company's cybersecurity controls.

SolarWinds published a Security Statement on its website, starting in 2017 and continuing through the company's IPO in 2018 and the cybersecurity incident in 2020, purporting to describe the

company's cybersecurity practices, which the SEC alleged contained five different sets of misrepresentations.

The court determined that false statements published on a company's website can sustain securities fraud liability even when the statements are directed at customers, not investors, because a public website is accessible to all, including investors, and as such is unavoidably part of the "total mix of information" that the company furnished to the investing public.

**What this means to you**

1. **Companies Must Ensure Public Statements about Cybersecurity Risks and Practices Are Accurate**

Public statements regarding cybersecurity can create securities fraud liability, particularly where the statements are detailed and specific about cybersecurity practices and risks. This includes statements directed at consumers (when available on a public website) and informal statements (such as blog posts or podcasts).

Given this, companies should review any public disclosures about their cybersecurity risks and practices to ensure the accuracy of these statements.

2. **The Exchange Act's Requirement to Maintain "Accounting Controls" Does Not Include Adoption of Cybersecurity Controls**

In the SolarWinds case, the court dismissed the argument that Section 13(b)(2)(B) of the Exchange Act requires companies to adopt cybersecurity controls to prevent unauthorized access to the company's computer systems.

This decision contrasts with the recent settlement by the SEC with R.R. Donnelley & Sons Co., a global provider of business communication and marketing services, which agreed to pay approximately $2.1 million to the SEC to settle alleged violations of Section 13(b)(2)(B) in connection with that company's response to a 2021 ransomware attack.

The court's SolarWinds decision may limit the SEC's future reliance on Section 13(b)(2)(B) to charge companies with alleged deficiencies in legal, compliance, or risk-management controls unrelated to corporate accounting. However, given that this decision represents only one federal district court's analysis of the issue, it remains uncertain whether the SEC will continue to pursue internal accounting controls violations under a theory of inadequate cybersecurity controls in other forums.

3. **Isolated Disclosure Failures Are Not Sufficient for a Finding of Inadequate Disclosure Controls and Procedures**

The court's dismissal of the SEC's Exchange Act Rule 13a-15 charge made clear that a disclosure controls and procedures violation requires "systemic deficiencies," not just one-off errors, particularly errors apparent principally in hindsight.

The reasoning in this case may be helpful to companies facing SEC criticism for discrete alleged lapses that occurred related to cybersecurity incidents notwithstanding a reasonably designed and implemented system of disclosure controls and procedures.

**Contact us**

Husch Blackwell's Securities & Corporate Governance team will continue to monitor the resolution of the remaining claims in this case and resulting implications for our clients. If you have any questions, please contact Craig Adoor, Steve Barrett, Robert Joseph, Victoria Sitz, Andrew Spector, Blake Heyer, or your Husch Blackwell attorney.