ALM | LAW.COM

THE AM LAW LITIGATION DAILY

Litigators of the (Past) Week: The SEC Walks Away From Its Case Against SolarWinds, Top Cybersecurity Officer

By Ross Todd
December 3, 2025

Late last month, the U.S. Securities and Exchange Commission agreed to dismiss claims that the software company concealed cyber vulnerabilities in the lead-up to the high-profile 2020 Sunburst attack. A team led by Sean Berkowitz and Serrin Turner of Latham & Watkins secured a ruling from a federal judge in Manhattan last year, gutting the SEC's case.

The enforcement action that the U.S. Securities and Exchange Commission brought in 2023 against SolarWinds captured the attention of the cybersecurity industry.

The SEC's suit, filed in the Southern District of New York, accused the Austin, Texas-based information technology software company and its chief information security office, Tim Brown, of concealing red flags in the run-up to the Sunburst attack in 2020 and misleading investors about the scope of the attack, which caused major disruptions to customers.

But our litigators of the week, **Sean Berkowitz** and **Serrin Turner** of **Latham & Watkins**, led a team that secured a ruling last year knocking the teeth out of the SEC's claims. U.S. District Judge Paul Engelmayer found that the SEC failed to show "actionable deficiencies" in the company's reporting and that claims about the company's post-hack statements "impermissibly rel[ied] on hindsight and speculation."

Courtesy photos

Serrin Turner (L) and Sean Berkowitz (R) of Latham & Watkins.

Late last month, the SEC agreed to dismiss its case against the company and Brown with prejudice, although the commission said the decision "does not necessarily reflect the Commission's position on any other case."

Who is your client and what was at stake here in this SEC action?

Serrin Turner: Our clients were SolarWinds, a leading developer of network monitoring software, and Tim Brown, its Chief Information Security Officer, who has a long and distinguished career in the cybersecurity field. What was at stake for both of them, beyond the threat of financial penalties and injunctive relief, was the potential reputational impact from the SEC's baseless allegations that they had misled SolarWinds investors about the company's security and had failed to implement basic security practices. For Tim in particular, the stakes were intensely personal, as Tim prides himself on being an advocate for strong cybersecurity and sought to be a model of transparency after the cyberattack SolarWinds experienced in 2020. Tim literally had a heart attack the day he learned of the SEC's charges. The desire to right the reputational wrongs that had been done to our clients was an abiding source of motivation for the Latham team throughout the case.

How did this matter come to you and the firm?

Sean Berkowitz: Before this case, Latham had no prior connection to SolarWinds and, in fact, SolarWinds was represented by another firm during the investigative phase of the case. When it appeared the case might end up in litigation, in-house counsel at SolarWinds solicited feedback from trusted colleagues at other public companies about who they would hire if they were going to fight, and potentially try a case against, the SEC. A general counsel at a large public company recommended me based on success I had previously had defeating the SEC in a major case for that company. I assembled a team that included Serrin, an expert in cybersecurity matters and a fellow former federal prosecutor, and after several rounds of interviews, SolarWinds' general counsel, Jason Bliss, and head of litigation, Becky Melton, chose to hire us to represent the company. We then spoke with Tim Brown, who decided to engage us as well, along with Alec Koch from King & Spalding serving as his shadow counsel—with SolarWinds paying for all of Tim's legal costs.

Who all was on the team and how have you divided the work?

Berkowitz: Our team was led by myself and Serrin, with a strong team of New York and Chicago-based associates, including **Matthew Valenti**, **Nicolas Luongo**, **Maurice Baynard** and **Christian Beveridge**, as well as former Latham associate **Kirsten Lee**. The team had an ideal blend of securities and cybersecurity experience. Our success was truly a team effort and demonstrated the best of what we can bring to bear in a high-stakes case like this. Serrin led the briefing in the case, while I was primarily responsible for negotiating with the SEC. We split oral argument on the motion to dismiss as well as the factual development during discovery. We were aided in our efforts not only by Alec Koch, but also by Andrew Ceresney and Anna Moody at Debevoise, who had represented the company during the investigative phase of the case. Most importantly, our partnership with the SolarWinds in-house legal team—led by Jason Bliss, Becky Melton, Anna Denton and Annie Gravelle—was instrumental in achieving the outcome we did.

Why did this particular case capture the attention of the cybersecurity world like it did?

Turner: I think what worried the cybersecurity community about this case was the overreaching regulatory agenda behind it. The SEC is not a cybersecurity regulator—it's neither congressionally authorized nor institutionally qualified to play such a role. Yet the SEC was clearly seeking to expand its regulatory sphere of influence over

cybersecurity through this enforcement action—pushing for cybersecurity disclosure obligations beyond anything the law previously required, and even claiming a general police power over public companies' cybersecurity controls, by falsely equating them with "accounting controls." Making matters worse, the SEC came up with the supposed evidence for its claims by sifting through the day-to-day communications of SolarWinds' IT staff and seizing on discussions of cybersecurity risks as if they were admissions of fraud. That understandably made cybersecurity professionals fearful that anything they said in their daily work—which constantly involves assessing risk—could be taken out of context by a regulator and used to target both their company and them personally. There was a real concern that this case would chill candid internal communication within cybersecurity programs as a result—harming the cause of cybersecurity rather than helping it.

You had multiple amicus groups back your position at the motion to dismiss phase. Who all joined that effort and how important do you think it was to this outcome?

Turner: Our amicus support was truly exceptional, and we are grateful to all who contributed, including software industry groups represented by Jim Garland at Covington, a collection of CISOs and CISO advocacy groups represented by Andrew Goldstein of Cooley and Tim Howard of Freshfields, the U.S. Chamber of Commerce and Business Roundtable represented by Nicole Friedlander at Sullivan & Cromwell, and a stellar roster of former government officials (even including a former SEC cyber enforcement chief!) represented by John Carlin at Paul Weiss. Their briefs powerfully explained how the SEC's aggressive legal theories threatened to disrupt and distort companies' cybersecurity operations if they became law. I have no doubt the briefs helped persuade Judge Engelmayer to reject those legal theories, as he did in dismissing most of the SEC's claims at the pleading stage.

What can other companies take from how SolarWinds approached this case?

Berkowitz: I hope that other companies will learn that you can fight the SEC and prevail if you have the facts and law on your side. It is always a risk to litigate against your primary regulator, and many companies make the understandable decision to settle rather than engage in a public fight with the government. Here, I give tremendous credit to Jason Bliss, Tim Brown and the company for recognizing the importance of this case, not only to Tim and the company, but also to the broader constituency of public companies and their CISOs nationwide. The company and Tim took a principled stand and placed their faith in the system, trusting that after the facts came to light, it would be apparent that nobody did anything wrong here. I think the approach they took and the ultimate outcome they achieved are valuable lessons for other companies facing similar choices in the future.

The SEC indicated that its decision to seek dismissal of the case "does not necessarily reflect the Commission's position on any other case." What lessons do you hope the agency has taken from this litigation?

Berkowitz: It took a lot of courage for the agency to walk away from this case after the public statements it made when the case was charged and the resources it expended over almost two years of actively litigating (and two years of investigating before that). I would hope the agency continues to keep an open mind on cases it charges and focuses on getting the right result based on the facts and law as they ultimately develop, rather than continuing to pursue

a case merely because they want to prevail. To paraphrase Justice Jackson, the government's role is to ensure justice is done, not merely to win a case.

Has handling this case made you rethink any of your own approaches to cybersecurity and digital hygiene?

Turner: No, it really hasn't—because the case wasn't genuinely about failures of cybersecurity hygiene. The SEC's complaint mischaracterized internal documents to *invent* cybersecurity hygiene failures that didn't actually exist. That is all laid out in our summary judgment briefing. However, what the case has caused cybersecurity lawyers to rethink is whether corporate legal departments should do more to supervise internal communications of cybersecurity personnel in order to minimize the potential for those communications to be misconstrued or misrepresented by regulators. I think some effort along those lines is advisable and have worked with companies on implementing processes for that. But I am wary of overlearning the lessons of this case and over-lawyering cybersecurity programs—which risks chilling candid internal communications and distorting program priorities. To my mind, the real lesson of this case is not for companies but for cybersecurity *regulators*: They should approach cybersecurity with more humility, taking care to learn all the relevant facts before bringing a case and to avoid jumping to conclusions based on hindsight or confirmation bias.

What will you remember most about this matter?

Berkowitz: Other than being able to celebrate in person with our client the day the SEC formally dismissed its case, the most memorable moment I had was when I was cross-examining the SEC's self-described whistleblower. The "whistleblower"—who was a marketing employee, not a cybersecurity employee—had very publicly claimed he warned SolarWinds about various supposed cybersecurity issues during his time at the company. After repeatedly showing the witness document after document about facts he was not aware of that contradicted his public statements, I asked him whether in fact he lacked sufficient information to support the allegations he had made. He answered: "This is becoming very apparent, yes."

Turner: While it may sound a little mundane, one of the things I will most remember is the joint statement of material facts we filed in support of our motion for summary judgment, where the SEC admitted—at long last—that SolarWinds routinely implemented the very controls the SEC's complaint had alleged the company pervasively neglected. Reaching that point required a great deal of work and effort during the discovery process, and it was satisfying to see the payoff in the form of a clear (albeit belated) admission of the truth from the SEC. I have to believe that the resulting cognitive dissonance—between what the SEC originally alleged and what they later conceded the facts showed—is what ultimately led the SEC to decide to dismiss the case altogether.