Cooley

Federal Court Dismisses Bulk of SEC's Complaint Against SolarWinds in Cyberattack Case

July 23, 2024

On July 18, 2024, US District Judge Paul Engelmayer of the Southern District of New York issued a detailed 107-page opinion and order dismissing most of the US Securities and Exchange Commission (SEC) case against SolarWinds and its chief information security officer (CISO). The SEC's amended complaint alleged that SolarWinds and its CISO misled investors through public statements and SEC disclosures before, during, and after a two-year-long Russian government-backed cyberattack campaign (dubbed "SUNBURST") against SolarWinds. The court dismissed three of five claims against SolarWinds and three of seven claims against its CISO.

Dismissed claims

First, the court dismissed all claims about the company's SEC filings prior to, during and after the SUNBURST cyberattack. The court found that the SEC's allegations about SolarWinds' disclosures in its annual and quarterly filings, as well as Form 8-K reports filed in response to SUNBURST, were not sufficient to support claims of security fraud or false filings.

Second, the court dismissed all claims that were based on press releases, blog posts, and podcasts by SolarWinds and its CISO regarding SolarWinds' cybersecurity policies and practices. The court concluded that those statements were non-actionable puffery, and the SEC had failed to plead sufficient detail to state a viable securities claim.

Third, the court dismissed all claims that SolarWinds maintained insufficient internal accounting and disclosure controls for cybersecurity. The court categorically rejected the SEC's theory that its authority to regulate internal accounting controls extends to a company's cybersecurity controls. The court referred to this category of claims as "ill-pled" and held that the SEC's statutory authority does not extend to regulating corporate cybersecurity.

The claims dismissed by Judge Engelmayer were noteworthy and novel in that they sought to:

1. Hold a CISO personally liable for a lack of detail in a company's SEC filings.
2. Base liability on a company's internal scoring against a nonbinding cybersecurity framework (the NIST Cybersecurity Framework).
3. Treat an issuer's cybersecurity practices as internal accounting controls.

The court's dismissal of these claims constitutes a significant victory for companies, their CISOs and cybersecurity. Earlier this year, Cooley filed an amicus brief on behalf of a coalition of more than 50 cybersecurity leaders and organizations. The brief highlighted fatal flaws in the SEC's amended complaint and explained how the SEC's novel and creative theories of liability (which the court rejected in its opinion) were "counterproductive given the real-world demands of cybersecurity, and risk harmful consequences, including elevating the frequency and harm of cyberattacks, impeding internal efforts to bolster cybersecurity, worsening the CISO hiring and retention crisis, and deterring CISOs from cooperating" with the government.

Other amici, including former law enforcement officials, raised similar arguments, and stressed that the SEC's claims could make companies more reticent to voluntarily share information with law enforcement, hampering government efforts to combat cyber threats. Judge Engelmayer's opinion echoed some of the concerns raised by Cooley and other amici. He noted, for example, that "spelling out a risk [in public filings] with maximal specificity may backfire in various ways, including by arming malevolent actors with information to exploit."

Some claims allowed to proceed

The court permitted a narrow category of more traditional claims against SolarWinds and its CISO to proceed. The court held that the SEC's allegations about SolarWinds' "Security Statement," and its CISO's involvement with it, were sufficiently detailed to support claims that investors were materially misled about the company's cybersecurity controls. The SEC alleged that the Security Statement – which SolarWinds published on its website in 2017 and maintained during the relevant period – contained misrepresentations about the company's access controls, password protections, compliance with the NIST Cybersecurity Framework, network monitoring, and implementation of a secure software development life cycle. The court held that the SEC had successfully pleaded that two of these representations were materially misleading to investors – those concerning access controls and password protections. The court explained that the SEC "plausibly allege[d]" that SolarWinds and its CISO misrepresented "the adequacy of [the company's] access controls," and that "[g]iven the centrality of cybersecurity to SolarWinds' business model as a company pitching sophisticated software products to customers for whom computer security was paramount, these misrepresentations were undeniably material."

Key points for companies and cybersecurity professionals

Despite dismissing the bulk of the SEC's complaint, the court's order counsels caution for companies, CISOs, their cybersecurity teams, and even marketing personnel, as to how they describe their cybersecurity policies and controls to investors and the public.

Security statement inventory

While the court dismissed some of SolarWinds' public statements as puffery, the "Security Statement" was still found actionable because it described SolarWinds' cybersecurity practices in enough detail for a reasonable investor to rely on. That statement also was allegedly contradicted by internal representations and communications within SolarWinds (including Slack and email messages, security reports, and assessment and audit results).

Cooley has been working with clients to inventory their public-facing statements around security. Targets include security whitepapers, security summaries/statements, ESG (environmental, social and governance) filings, marketing materials and, of course, financial statements. We've found that organizations like to talk about their security a lot, usually as a selling point or to establish credibility for their service offering. In fact, establishing sound security practices is often a threshold issue for closing deals with customers. Companies should consider undertaking a global inventory of their public statements about their cybersecurity functions and controls and a review for accuracy and consistency.

Going forward, companies also should consider whether their statements on security may constitute information on which investors may rely and, if so, apply appropriate review and public disclosure control processes to such statements. This would include processes to ensure that security-related statements to be issued by the company accurately describe – and do not overstate – its cybersecurity function, controls, and policies. Companies should carefully consider whether any content of such statements could be considered false, incomplete, or misleading to investors and the public, and whether these statements are consistent across the mediums and channels through which the company communicates.

Collaboration and communication between security function and relevant business stakeholders

Companies should open lines of communication between CISOs and management to break down silos hampering risk assessment and mitigation. The court allowed the securities fraud claim against SolarWinds' CISO to proceed, which, as noted in Cooley's amicus brief, could give CISOs and cybersecurity professionals an incentive to prioritize avoiding potential personal liability rather than focus on their company's cybersecurity. Companies can combat this potential by encouraging effective communications between cybersecurity professionals and the CISO, as well as between the CISO and senior management, the board of directors, and other nonsecurity stakeholders.

Security team training on internal security-related communications

The claims surviving the motion to dismiss are based in large part on alleged inconsistencies between the internal communications of SolarWinds' CISO and security team, and the content of their security statement. While open and frank communications about security challenges are necessary, informal, sloppy, or inflammatory communications can be harmful (and ultimately ineffective). Now, more than ever, security professionals need to know how to appropriately communicate to achieve their objectives. This not only increases the effectiveness of security teams but also reduces the risk of liability (including personal liability of security professionals). Cooley has developed training specifically targeted at security professionals to foster

clear, concise, and complete internal communications on cybersecurity vulnerabilities and priorities. It addresses communicating using informal channels, drafting appropriate security reports, understanding the regulatory and legal context where communications are scrutinized, and prioritizing accuracy and completeness to obtain positive outcomes for the security team and their organization.

If you have questions or concerns about the impact of this ruling on your business, contact one of the Cooley lawyers listed below.

Cooley counsels corporate and individual clients on all aspects of cybersecurity – including strategy, governance, risk management, disclosures, incident response, investigations, and enforcement actions.

In the event of a suspected data incident, members of Cooley's 24/7 data incident and breach response team can be reached at any time using the contact information below.

Cooley Incident Response Hotline
cyber/data/privacy
incident.response@cooley.com
+1 844 476 1248
+ 1 415 693 2888

For additional resources, visit Cooley's SEC Cybersecurity Disclosure Rules Resources page.

Key Contacts

Andrew D. Goldstein **Washington, DC**	**agoldstein@cooley.com** **+1 202 842 7805**
Travis LeBlanc Washington, DC	tleblanc@cooley.com +1 202 728 7018
Michael Egan Washington, DC	megan@cooley.com +1 202 776 2249
Mari Dugas New York	mdugas@cooley.com +1 202 740 0747

Matt K. Nguyen Washington, DC	mnguyen@cooley.com +1 202 728 7123