BLANKROME

Privacy, Security & Data Protection

JULY 29, 2024

Court Dismisses Most of SEC's Cyber Case Against SolarWinds

In an impactful decision that may limit the scope of future Securities and Exchange Commission ("SEC") enforcement efforts against public companies over inadequate cyber controls, the U.S. District Court for the Southern District of New York recently dismissed significant portions of the SEC's fraud and internal accounting controls case against software developer SolarWinds Corp. ("SolarWinds"). The lawsuit focused on a series of cyber-attacks against SolarWinds beginning in 2020. Those attacks (collectively, "SUNBURST") introduced vulnerabilities into SolarWinds' software, causing widespread data breaches among SolarWinds customers. In light of this decision, companies, especially those selling technology products/services, should analyze their public statements for accuracy and completeness regarding the capabilities and controls in their cyber systems.

The SEC's complaint includes allegations of (1) insufficient disclosures following discovery of the SUNBURST incident, (2) failure to implement appropriate internal accounting controls as required by the Exchange Act, and (3) fraudulent disclosures regarding SolarWinds' cybersecurity program.

Regarding the first of these allegations—risk disclosures concerning the SUNBURST incident—the court rejected the SEC's claim that SolarWinds failed to accurately report the initial stages of the SUNBURST incident in 2020. The court found no authority "supporting a legal duty to update [SolarWinds'] risk disclosure" where it had not definitively linked two pre-existing data security incidents to reveal a more significant vulnerability prior to the SUNBURST incident, holding that such allegations "impermissibly rely on hindsight and speculation." The court also dismissed the SEC's claim that SolarWinds' post-SUNBURST risk disclosure in its Form 8-K was materially misleading, finding that the disclosure was made when SolarWinds' understanding of the incident was evolving.

Similarly, the court rejected the SEC's novel argument that SolarWinds' cybersecurity deficiencies constituted a failure to "device and maintain a system of internal accounting controls" as defined in Section 13(b)(2)(B) of the Exchange Act. In dismissing these claims as "ill-plead," the court found that while an issuer's "system of internal accounting controls" requires the issuer accurately report, record, and reconcile financial transactions, it "cannot reasonably be interpreted to cover a company's cybersecurity controls such as its password and VPN controls."

Despite these significant victories, the court did permit the SEC to proceed with its fraud claim relating to SolarWinds' statements about its cybersecurity program. The SEC alleged that SolarWinds and its Chief Information Security Officer ("CISO") "knew, between 2017 and 2020,

that its cybersecurity apparatus was deeply flawed[,]" pointing to multiple internal reports and presentations highlighting security deficiencies. Despite these known deficiencies, SolarWinds and its CISO allegedly published multiple statements misrepresenting the status of its cybersecurity program, including a Security Statement on the Trust Center of the SolarWinds website. These included representations that SolarWinds "follows the NIST Cybersecurity Framework" despite an assessment demonstrating that they had substantial areas where little or no controls were in place. Further SolarWinds' primary business is information system security. The court noted these misstatements were significant as "SolarWinds' cybersecurity practices were central to its ability to obtain and retain business." Therefore, the court sustained the SEC's theories of fraud liability with respect to SolarWinds' pre-SUNBURST statement.

On its whole, however, the Southern District of New York's opinion is a significant "'win" for SolarWinds and may impact the SEC's efforts to pursue other enforcement actions premised on a company's failure to implement adequate cyber controls. Public companies may also take some solace in the court's sympathetic view of SolarWinds' risk disclosures issued during a rapidly unfolding security incident.

For more information and assistance, contact Philip N. Yannella, Sharon R. Klein, Timothy W. Dickens, Jason C. Hirsch, or another member of Blank Rome's Privacy, Security & Data Protection group.

Philip N. Yannella
215.569.5506 | philip.yannella@blankrome.com

Sharon R. Klein
949.812.6010 | sharon.klein@blankrome.com

Timothy W. Dickens
215.569.5352 | timothy.dickens@blankrome.com

Jason C. Hirsch
215.569.5445| jason.hirsch@blankrome.com