

Internal Accounting Controls Claim Rejected in SolarWinds Case

July 23, 2024

On July 18, 2024, in the landmark *SEC v. SolarWinds Corp.* case, U.S. District Judge Paul Engelmayer dismissed the majority of the claims brought by the U.S. Securities and Exchange Commission (the “SEC”) against SolarWinds Corporation (“SolarWinds”), including the SEC’s previously untested claim that alleged deficiencies in SolarWinds’ cybersecurity controls amounted to violations of the internal accounting controls requirements of Section 13(b)(2)(B) of the Securities Exchange Act of 1934.

The SEC’s internal accounting controls claim against SolarWinds presented the first opportunity for a federal court to evaluate the SEC’s theory that Section 13(b)(2)(B) could be extended beyond financial accounting controls, as they were traditionally understood, to include cybersecurity controls related to technology assets more generally. The SEC had alleged that SolarWinds violated Section 13(b)(2)(B) by allegedly failing to “devise and maintain a system of internal accounting controls” to limit access to its “crown jewel” assets, including key software products and associated systems.

As we wrote about last month in our article [“Incident Response Plans Are Now Accounting Controls? SEC Brings First-Ever Settled Cybersecurity Internal Controls Charges,”](#) the SEC recently settled similar charges against communications and marketing provider R.R. Donnelley & Sons Co. (“RRD”). There, the SEC’s settled order found that RRD had violated Section 13(b)(2)(B) by allegedly failing to implement a “system of cybersecurity-related internal accounting controls” sufficient to provide reasonable assurances that access to the company’s assets—namely, its information technology systems and networks—was permitted only with management’s authorization. RRD agreed in the no-admit, no-deny settlement to pay a \$2.125 million penalty to resolve the charges, which arose from its response to a 2021 ransomware attack.

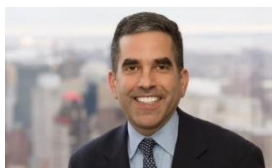
In *SolarWinds*, the court found that the SEC’s attempt to expand Section 13(b)(2)(B) was an impermissible overreach. The court held that the cybersecurity controls at issue in the SEC’s suit against SolarWinds, such as password and VPN protocols, are “outside the scope of Section 13(b)(2)(B)” because they “cannot reasonably be termed an

accounting problem.” Tracing the origins of the internal accounting controls requirements to the 1977 passage of the Foreign Corrupt Practices Act (the “FCPA”), [the opinion](#) held that Section 13(b)(2)(B) was “intended to provide extra assurance of the accuracy and completeness of the financial information on which the issuer’s annual and quarterly reports rely.” Noting also that the FCPA was adopted “long before cybersecurity became a relevant concept in business or society,” the court concluded that an issuer’s cybersecurity controls were not part of the “apparatus” required by Section 13(b)(2)(B).

The SEC’s expansive approach in applying Section 13(b)(2)(B) beyond financial accounting controls, including in other contexts arguably beyond the scope defined by the court (such as 10b5-1 plans), has been controversial, even within the SEC. SEC Commissioners Hester Peirce and Mark Uyeda issued a blistering [dissenting statement](#) to the RRD settlement, arguing that the SEC has in recent years inappropriately treated “Section 13(b)(2)(B)’s internal accounting controls provision as a Swiss Army Statute to compel issuers to adopt policies and procedures the Commission believes prudent.”¹ It remains to be seen if the court’s decision in *SolarWinds* will cause the SEC to temper its aggressive approach on this issue. Regardless, as a practical matter, the court’s decision may limit one of the SEC’s tools to bring charges in cybersecurity and other disclosure cases without alleging fraud under Section 10(b) of the Securities Exchange Act of 1934 or Section 17(a) of the Securities Act of 1933.

* * *

Please do not hesitate to contact us with any questions.



Andrew J. Ceresney
Partner, New York
+1 212 909 6947
aceresney@debevoise.com



Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandrasekhar@debevoise.com



Luke Dembosky
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com

¹ SEC Commissioners Peirce and Uyeda had previously dissented in the SEC’s settlement with Charter Communications, Inc. and called the SEC’s expansive approach in applying Section 13(b)(2)(B) “the Commission’s attempts to convert an internal accounting controls provision into an ever-unfolding utility tool that magically converts every corporate activity into something the Commission regulates.” Statement of Commissioners Hester M. Peirce and Mark T. Uyeda, *The SEC’s Swiss Army Statute: Statement on Charter Communications, Inc.* (Nov. 14, 2023), available at <https://www.sec.gov/news/statement/peirce-uyeda-statement-charter-communications-111423>.



Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com



Benjamin R. Pedersen
Partner, New York
+1 212 909 6121
brpedersen@debevoise.com



Julie M. Riewe
Partner, Washington, D.C.
+1 202 383 8070
jriewe@debevoise.com



Paul Rodel
Partner, Washington, D.C.
+1 212 909 6478
pmrodel@debevoise.com



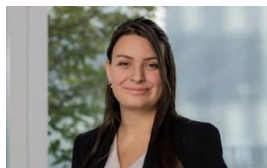
Matt Kelly
Counsel, New York
+1 212 909 6990
makelly@debevoise.com



Anna Moody
Counsel, Washington, D.C.
+1 202 383 8017
amoody@debevoise.com



Alice Gu
Associate, New York
+1 212 909 6057
agu@debevoise.com



Talia Lorch
Associate, New York
+1 212 909 6707
tnlorch@debevoise.com

This publication is for general information purposes only. It is not intended to provide, nor is it to be used as, a substitute for legal advice. In some jurisdictions it may be considered attorney advertising.