Proskauer

SolarWinds Government Data Breach Leads to Securities Action

Corporate Defense and Disputes Blog on **January 6, 2021**

The massive data breach of the United States Commerce and Treasury Departments that has roiled the federal government has resulted in federal securities litigation. On January 4, 2021, Plaintiff-Shareholder Timothy Bremer filed a class action complaint against SolarWinds and SolarWinds' corporate executives in the United States District Court for the Western District of Texas. SolarWinds provides information technology and infrastructure management software products to entities around the globe, including to various U.S. government vendors in the executive branch, military, and intelligence services. According to the complaint, Russian hackers gained access to government email traffic by deceptively interfering with software updates released by SolarWinds. The complaint alleges that SolarWinds violated federal securities law by making false and/or misleading statements and failing to disclose material facts regarding SolarWinds' cybersecurity practices and protocols, which artificially inflated the market price of SolarWinds' shares. When news of the hack became public, the value of Solarwinds' securities dropped, thereby producing an economic loss for investors within the class period of February 24, 2020 through December 15, 2020. The complaint asserts claims for violations of Section 10(b) of the Securities Exchange Act of 1934 (the "Exchange Act") and Rule 10b-5 against SolarWinds and its corporate executives, and for violations of Section 20(a) of the Exchange Act against the corporate executives.

To establish securities fraud under Rule 10b-5, a plaintiff must show (1) a material misrepresentation or omission (2) made with scienter (3) in connection with the purchase or sale of a security; (4) reliance on the misrepresentation or omission; (5) economic loss; and (6) loss causation. *Dura Pharmaceuticals v. Broudo*.

According to the complaint, SolarWinds failed to disclose that it had a security vulnerability—an easily accessible password—which allowed hackers to compromise the server and made its customers vulnerable to cyberattacks. Notwithstanding this knowledge, the complaint alleges that SolarWinds' 2019 Form 10-K and Form 10-Qs for the first three quarters of 2020 were materially false and misleading because they stated, among other things, that "[t]he risk of a security breach or disruption, particularly through cyberattacks or cyber intrusion, including by computer hacks, foreign governments, and cyber terrorists, has generally increased the number, intensity and sophistication of attempted attacks, and intrusions from around the world have increased." Plaintiff alleges that these disclosures were insufficient because they failed to discuss the significant cybersecurity risk to the company and its clients caused by SolarWinds' vulnerabilities.

The complaint alleges that the truth came to light beginning with a December 13, 2020 *Reuters* report that hackers alleged to be working for the Russian government gained access to the U.S. Treasury and Commerce departments' emails by deceptively interfering with SolarWinds' product updates. The next day, SolarWinds filed a Form 8-K with the Securities and Exchange Commission disclosing that it had been subject to the cyberattack. SolarWinds' shares fell 17% on this news. The next day, *Reuters* published another article stating that in 2019, a security researcher notified SolarWinds that anyone could access SolarWinds' update server by using the password "solarwinds123." The same day, SolarWinds' shares fell 8%.

Lead counsel has not yet been designated. After a lead plaintiff is appointed, we can expect an amended complaint to be filed with additional allegations. It also remains to be seen whether the government will seek any damages against SolarWinds for its role in the massive cyberattack. Follow along here for additional updates.

View Original

Related Professionals

- **Brooke G. Gottlieb**
  Associate