Securities Regulation Daily Wrap Up, FRAUD AND MANIPULATION—N.D. Cal.: New lawsuits zero in on Zoom's alleged data security failures, (Apr. 13, 2020)

Securities Regulation Daily Wrap Up

Click to open document in a browser

By John M. Jascob, J.D., LL.M.

Investors accuse the video conferencing provider of covering up weaknesses in its data privacy and security measures that were exposed by the onset of COVID-19.

Two new shareholder suits have charged Zoom Video Communications, Inc. with misrepresenting the data security of its video conferencing services. In separate class action complaints filed in federal court in San Francisco, investors allege that the company violated Exchange Act Section 10(b) and Rule 10b-5 by significantly overstating the degree to which its video communication software was encrypted. Once the company's obfuscations about its encryption became clear following the increasing reliance on video conferencing during the COVID-19 pandemic, the complaints allege, businesses prohibited employees from using Zoom's platform, causing the company's share price to plummet (*Drieu v. Zoom Communications, Inc.*, April 7, 2020; *Brams v. Zoom Video Communications, Inc.*, April 8, 2020).

Zoom. Founded in 2011 and headquartered in Silicon Valley, Zoom provides a cloud-based communications application that allows users to interact with each other by means of face-to-face video, audio, and chat. On April 17, 2019, the registration statement for Zoom's initial public offering (IPO) was declared effective by the SEC.

According to the complaints, Zoom, CEO Eric Yuan, and CFO Kelly Steckelberg made materially false and misleading statements regarding the company's business, operational, and compliance policies, both in connection with the IPO and in subsequent filings with the SEC.

Contrary to Zoom's assertions, the shareholders claim, Zoom's video communications service was not end-to-end encrypted, thus putting users at an increased risk of having their personal information accessed by unauthorized parties. A decline in the use of Zoom's video communications services was foreseeably likely when these facts came to light, the complaints allege, making Zoom's SEC filings and public statements materially false and misleading at all relevant times.

Pomerantz lawsuit. The complaint filed by the Pomerantz law firm alleges that the truth began to emerge on July 8, 2019, when security researcher Jonathan Leitschuh posted on Twitter a link to an article he had published, which allegedly exposed a flaw allowing hackers to take over Zoom webcams. Just three days later, the Electronic Privacy Information Center (EPIC) filed a complaint against Zoom with the Federal Trade Commission, alleging that Zoom had intentionally designed their web conferencing service to bypass browser security settings for webcams, exposing users to the "risk of remote surveillance, unwanted videocalls, and denial-of-service attacks." Despite these disclosures, however, Zoom's stock continued to trade at artificially inflated levels, the complaint alleges.

The Pomerantz complaint alleges that the truth fully emerged, however, as businesses increasingly turned to Zoom's video communication software to facilitate remote work activity in the midst of the COVID-19 pandemic and shelter-in-place orders from state and local governments. For example, the *New York Times* reported on March 30, 2020, that Zoom was under scrutiny by the New York attorney general for its data privacy and security practices. According to the article, the attorney general's investigation cited, among other things, Leitschuh's findings regarding webcam security issues, the complaint filed with the FTC, and revelations from an article by Vice Media's *Motherboard* segment that the iOS version of the Zoom app was sending some analytics data to Facebook, even if Zoom users didn't have a Facebook account. The *New York Times* article also

reported that "trolls have exploited a Zoom screen-sharing feature to hijack meetings and do things like interrupt educational sessions or post white supremacist messages to a webinar on anti-Semitism—a phenomenon called 'Zoombombing.'"

After additional negative news, the Pomerantz complaint states, New York City's Department of Education announced on April 6, 2020, that it had banned the use of Zoom in the city's classrooms. Instead, the Department recommended Google or Microsoft Teams for classroom communications purposes during New York State's shelter-in-place order. That same day, a *Yahoo! Finance* article reported that someone on a popular dark web forum had posted a link to a collection of 352 compromised Zoom accounts. According to a spokesperson for the cybersecurity firm Sixgill who was quoted in the article, "these links included email addresses, passwords, meeting IDs, host keys and names, and the type of Zoom account," and that, "given that many are using Zoom for business purposes, confidential information could be compromised."

As a result of the defendants' wrongful acts and omissions, the complaints assert, the plaintiffs and other class members have suffered significant losses and damages.

The cases are No. 20-cv-02353 (*Drieu*) and No. 20-cv-02396 (*Brams*).

Attorneys: James Matthew Wagstaffe (Wagstaffe, Von Loewenfeldt, Busch & Radwick LLP) for Kim Brams. Jennifer Pafiti (Pomerantz LLP) for Michael Drieu.

Companies: Zoom Video Communications, Inc.

LitigationEnforcement: Covid19 CyberPrivacyFeed DataBreach FraudManipulation NewLawsuitsNews CaliforniaNews