June 21, 2024

SEC Charges Company with Internal Accounting Controls Failure Based on Cybersecurity Breach

Action Shows SEC's Expansive Interpretation of Its Authority Under the Internal Accounting Controls Provision of the Exchange Act

SUMMARY

On June 18, 2024, the Securities and Exchange Commission ("SEC") announced charges against R.R. Donnelley & Sons Company ("RRD") for failure to maintain adequate internal accounting controls in violation of Section 13(b)(2)(B) of the Securities Exchange Act of 1934 ("Exchange Act"), and failure to maintain adequate disclosure controls and procedures in violation of Exchange Act Rule 13a-15(a).[1] The charges, which were simultaneously settled pursuant to a cease-and-desist order (the "Order")[2] imposing a $2,125,000 civil penalty, stemmed from RRD's allegedly inadequate policies and procedures that led to RRD's failure to execute a timely response to a ransomware network intrusion that culminated in encryption of computers, exfiltration of data, and business service disruptions.

This action represents the SEC's latest assertion of jurisdiction under Section 13(b)(2)(B) of the Exchange Act to punish a company for alleged failures that do not impact the company's financial reporting or accounting controls. It is the second action in which the SEC has used the provision to fault a company after the company was compromised in a cyber attack. The first action, against SolarWinds Corporation, is currently being litigated in the United States District Court for the Southern District of New York, where the SEC's expansive interpretation of the provision is being challenged.

Two SEC Commissioners dissented from the SEC's decision to charge RRD under Section 13(b)(2)(B), repeating a view they expressed in recent prior dissents that the SEC lacks jurisdiction under the provision to charge companies for alleged "control failures" that do not involve accounting controls in particular. In

light of this enforcement action, companies should be mindful that the SEC is continuing to pursue its expansive reading of Section 13(b)(2)(B), including in situations in which companies have been victimized by cybercrime.

RELEVANT EXCHANGE ACT PROVISIONS

Section 13(b)(2)(B) of the Exchange Act requires publicly traded companies to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that—(i) transactions are executed in accordance with management's general or specific authorization; (ii) transactions are recorded as necessary (I) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (II) to maintain accountability for assets; (iii) access to assets is permitted only in accordance with management's general or specific authorization; and (iv) the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences."[3]

Rule 13a-15(a) of the Exchange Act requires that covered issuers maintain disclosure controls and procedures "that are designed to ensure that information required to be disclosed by the issuer in the reports that it files or submits under the Act . . . is recorded, processed, summarized and reported, within the time periods specified" by the SEC.[4] These controls and procedures must ensure that information required to be disclosed is communicated to senior management.[5]

BACKGROUND

R.R. Donnelley & Sons Company is a global provider of business communication and marketing services. The Order alleges that information technology and cybersecurity are critically important to RRD due to its business of storing and transmitting large amounts of data, including sensitive client data such as business plans and personally identifying and financial information of customers.[6]

According to the Order, as a result of RRD's internal accounting controls deficiencies, RRD failed to execute a timely response to a ransomware network intrusion that occurred between November 29, 2021 and December 23, 2021, which "culminated in encryption of computers, exfiltration of data, and business service disruptions."[7] Specifically, the Order found that while RRD's internal systems began issuing alerts on the first day of the compromise, roughly three weeks before any encryption and exfiltration of data took place, "RRD's external and internal security personnel failed to adequately review these alerts and take adequate investigative and remedial measures until a company with shared access to RRD's network notified RRD about anomalous internet traffic on December 23, 2021."[8] RRD's investigation found no evidence, however, that RRD's own financial systems and corporate financial or accounting data were accessed.[9]

The SEC premised its Section 13(b)(2)(B) charge on criticisms of RRD's cyber incident response policies and procedures and RRD's processes for reviewing alerts for potentially malicious cyber activity which,

according to the SEC, "failed to adequately establish a prioritization scheme and to provide clear guidance to internal and external personnel on procedures for responding to incidents."[10] In addition, according to the SEC, RRD "failed to establish sufficient internal controls to oversee its third-party managed security services provider's review and escalation of the alerts."[11]

SEC Commissioners Hester Pierce and Mark T. Uyeda dissented to the Order, criticizing the SEC's apparent "plans to dictate public company cybersecurity practices indirectly using its ever-flexible Section 13(b)(2)(B) tool." As the Commissioners noted, the "assets" that the hackers accessed were RRD's "information technology systems and networks," which "are not an asset of the type covered by Section 13(b)(2)(B)'s internal accounting controls provisions."[12] In that regard, the Order "breaks new ground with its expansive interpretation of what constitutes an asset under Section 13(b)(2)(B)(iii)" and "ignores the distinction between internal accounting controls and broader administrative controls."[13] Critically, they observed:

> Eliding the distinction between administrative controls and accounting controls has utility for the Commission. As this proceeding illustrates, a broad interpretation of Section 13(b)(2)(B) to cover computer systems gives the Commission a hook to regulate public companies' cybersecurity practices. Any departure from what the Commission deems to be appropriate cybersecurity policies could be deemed an internal accounting controls violation. . . . Also concerning is the Commission's decision to stretch the law to punish a company that was the victim of a cyberattack. While an enforcement action may be warranted in some circumstances, distorting a statutory provision to form the basis for such an action inappropriately amplifies a company's harm from a cyberattack.[14]

This is the third Section 13(b)(2)(B) action from which SEC Commissioners have dissented on the ground that the SEC has exceeded its jurisdiction by charging companies based on alleged "control failures" that are unrelated to accounting controls. Last year, for example, the same Commissioners dissented from the SEC's use of the internal accounting controls provision to charge Charter Communications based on an alleged deficiency in legal and compliance controls.

IMPLICATIONS

The SEC's broad reading of its authority under Section 13(b)(2)(B) in the RRD and SolarWinds actions has particular ramifications for companies dealing with cybersecurity breaches. As the dissenting Commissioners asserted with respect to the RRD action, this broad reading "gives [the SEC] a hook to regulate public companies' cybersecurity practices." Specifically, the logic it relies on—*i.e.*, that companies' information systems are assets under Section 13(b)(2)(B) such that, if the systems are accessed without authorization, the SEC may assert a violation of Section 13(b)(2)(B) by the company—will apply in every case in which a company experiences a cybersecurity breach.

Given the pending challenge in the *SolarWinds* case to the SEC's expansive interpretation of its jurisdiction under Section 13(b)(2)(B), it remains to be seen whether the SEC's use of the provision to penalize companies victimized by cybercrime will withstand judicial scrutiny.

* * *

ENDNOTES

1 U.S. Securities & Exchange Commission, Press Release, *SEC Charges R.R. Donnelley & Sons Co. with Cybersecurity-Related Controls Violations* (June 18, 2024), *available at* https://www.sec.gov/news/press-release/2024-75.

2 *In the Matter of R.R. Donnelley & Sons Co.*, Release No. 100365 (June 18, 2024), *available at* https://www.sec.gov/files/litigation/admin/2024/34-100365.pdf [hereinafter, Order].

3 Exchange Action Section 13(b)(2)(B).

4 Exchange Act Rule 13a-15(a), (e).

5 *Id.*

6 Order at ¶ 1.

7 *Id.*

8 Order at ¶ 17.

9 Order at ¶ 13.

10 Order at ¶ 16.

11 *Id.*

12 U.S. Securities & Exchange Commission, Statement, *Hey, look, there's a hoof cleaner! Statement on R.R. Donnelley & Sons, Co.* (June 18, 2024), *available at* https://www.sec.gov/news/statement/peirce-uyeda-statement-rr-donnelley-061824.

13 *Id.*

14 *Id.*

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 900 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.