UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 100365 / June 18, 2024

ADMINISTRATIVE PROCEEDING
File No. 3-21969

In the Matter of

R.R. DONNELLEY & SONS CO.

Respondent.

ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS, PURSUANT TO SECTION 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING A CEASE-AND-DESIST ORDER

I.

The Securities and Exchange Commission ("Commission" or "SEC") deems it appropriate that cease-and-desist proceedings be, and hereby are, instituted pursuant to Section 21C of the Securities Exchange Act of 1934 ("Exchange Act") against R.R. Donnelley & Sons Co. ("RRD" or "Respondent").

II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer") which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over it and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Cease-and-Desist Proceedings Pursuant to Section 21C of the Exchange Act of 1934, Making Findings, and Imposing a Cease-And-Desist Order ("Order"), as set forth below.

III.

On the basis of this Order and Respondent's Offer, the Commission finds that:

Summary

1. This matter concerns violations by RRD of the Exchange Act's disclosure controls and procedures and internal accounting control provisions relating to its cybersecurity practices between November 2021 and January 2022 (the "Relevant Period"). Throughout the Relevant Period, RRD failed to design effective disclosure controls and procedures as defined in the Exchange Act rules related to the disclosure of cybersecurity risks and incidents. RRD also failed to devise and maintain a system of cybersecurity-related internal accounting controls sufficient to provide reasonable assurances that access to RRD's assets – its information technology systems and networks, which contained sensitive business and client data – was permitted only with management's authorization. Due to RRD's business of storing and transmitting large amounts of data, including sensitive data, information technology and cybersecurity are critically important to RRD. As a result of these 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.

2. Based on the foregoing conduct, and the conduct described herein below, RRD violated Exchange Act Section 13(b)(2)(B) and Rule 13a-15(a).

Respondent

3. RRD, a Delaware corporation with headquarters in Chicago, Illinois, is a global provider of business communications services and marketing solutions. From August 2016 until February 2022, RRD was a publicly-traded company whose stock was traded on the New York Stock Exchange ("NYSE") under the ticker symbol RRD. RRD's stock was also traded on the National Association of Securities Dealers Automated Quotations ("NASDAQ") between August 2009 and August 2016. In connection with these listings, RRD's common stock was registered under Section 12(b) of the Exchange Act. On February 28, 2022, the NYSE filed a notice under Form 25 striking from listing and terminating RRD's registration of common shares. Between 2009 and 2022, RRD was required to file with the Commission annual reports on Forms 10-K and quarterly reports on Forms 10-Q pursuant to Section 13(a) of the Exchange Act and related rules thereunder.

4. As part of its services, RRD's information technology network regularly stored and transmitted data of its clients, which included SEC-registered firms, healthcare organizations, publicly-traded companies, and financial institutions. RRD's clients regularly provided RRD with confidential data and information, including business plans and personal identifying and financial information of their customers, in order to use RRD's services.

Facts

RRD's Security Incident Management

5. During the Relevant Period, RRD's internal intrusion detection systems issued a significant number of alerts each month. These alerts and the environment from which they emanated were highly complex due to RRD's large footprint and heterogeneity of its network and the variety of custom applications used in the environment. These alerts were available to RRD's internal personnel for review, but were reviewed in the first instance by its third-party managed security services provider (the "MSSP"). After initial review and analysis, the MSSP would escalate a significant number of alerts to RRD's internal cybersecurity personnel. When incidents of unauthorized activity were identified, the response and remediation were executed by both RRD's internal personnel and the MSSP.

6. Despite the high volume and complexity of the alerts the MSSP was responsible for reviewing, RRD did not reasonably manage the MSSP's allocation of resources to the task. In its contract and communications with the MSSP, RRD failed to reasonably set out a sufficient prioritization scheme and workflow for review and escalation of the alerts.

7. RRD did not have sufficient procedures to audit or otherwise oversee the MSSP in order to confirm that the MSSP's review and escalation of the alerts was consistent with RRD's expectations and instructions.

8. Despite the high volume and complexity of the alerts the MSSP escalated to RRD, the staff members allocated to the task of reviewing and responding to these escalated alerts had significant other responsibilities, leaving insufficient time to dedicate to the escalated alerts and general threat-hunting in RRD's environment.

9. RRD's internal policies governing its personnel's review of cybersecurity alerts and incident response also failed to sufficiently identify lines of responsibility and authority, set out clear criteria for alert and incident prioritization, and establish clear workflows for alert review and incident response and reporting.

2021 Ransomware Incident

10. Between November 29 and December 23, 2021, RRD experienced a ransomware network intrusion ("2021 Ransomware Intrusion"). Starting November 29, 2021, RRD's internal intrusion detection systems began issuing alerts, which were visible to both its and the MSSP's security personnel, about certain malware in the RRD network. The MSSP received these alerts and escalated three of them to RRD's internal security personnel. In the escalated alerts, the MSSP noted to RRD: (1) the indications that similar activity was taking place on multiple computers (meaning, the threat had moved laterally or the threat actors successfully achieved entry at multiple points); (2) connections to a broad phishing campaign; and (3) open-source intelligence that the malware was capable of facilitating remote execution of arbitrary code. The MSSP provided to

RRD a link to a cybersecurity magazine article, which described the malware and stated that it was often used in ransomware operations.

11. RRD reviewed the escalated alerts but, in partial reliance on its MSSP, did not take the infected instances off the network and failed to conduct its own investigation of the activity, or otherwise take steps to prevent further compromise, before December 23, 2021.

12. In November and December 2021, the MSSP also reviewed, but did not escalate to RRD, at least 20 other alerts related to the same activity, including alerts regarding the same malware being installed or executed on multiple other computers across the network and compromise of a domain controller server, which provided the threat actor with access to and control over a broader sweep of network resources and credentials. The malware executed on the domain controller was at the time publicly known to have been used by the ransomware group credited with the attack on RRD.

13. Between November 29 and December 23, 2021, the threat actor was able to utilize deceptive hacking techniques to install encryption software on certain RRD computers (mostly virtual machines) and exfiltrated 70 Gigabytes of data, including data belonging to 29 of RRD's 22,000 clients, some of which contained personal identification and financial information. RRD's investigation uncovered no evidence that the threat actor accessed RRD's financial systems and corporate financial and accounting data.

14. RRD began actively responding to the attack on December 23, 2021 after a company with shared access to RRD's network alerted RRD's Chief Information Security Officer about potential anomalous internet activity emanating from RRD's network. After this alert, RRD's security personnel conducted a rapid and extensive response operation, including shutting down servers, and notifying clients and federal and state agencies. Beginning on December 27, 2021, RRD issued public statements, including in EDGAR filings, regarding the 2021 Ransomware Intrusion.

RRD's Failure to Maintain Sufficient Internal Accounting Controls and Disclosure Controls and Procedures

15. Despite the importance of data integrity and confidentiality to RRD, RRD failed to design effective disclosure-related controls and procedures around cybersecurity incidents to ensure that relevant information was communicated to management to allow timely decisions regarding potentially required disclosure. For example, RRD's cybersecurity procedures and controls were not designed to ensure all relevant information relating to alerts and incidents was reported to RRD's disclosure decision-makers in a timely manner, and did not provide guidance regarding the personnel responsible for reporting such information to management. As a result, despite having information regarding the 2021 Ransomware Intrusion from RRD's detection systems and its cybersecurity service provider, RRD failed to adequately assess such information from a disclosure perspective.

16. RRD failed to reasonably design and maintain internal controls that complied with Exchange Act Section 13(b)(2)(B). Namely, as discussed above, RRD's cybersecurity alert review and incident response policies and procedures failed to adequately establish a prioritization scheme and to provide clear guidance to internal and external personnel on procedures for responding to incidents. In addition, RRD failed to establish sufficient internal controls to oversee the MSSP's review and escalation of the alerts.

17. During the 2021 ransomware incident, RRD's failure to design and maintain internal controls sufficient to provide reasonable assurances that access to RRD's assets was permitted only with management's authorization was exploited by hackers. While RRD's internal systems began issuing alerts on the first day of the compromise, approximately 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.

Violations

18. As a result of the conduct described above, RRD violated Exchange Act Section 13(b)(2)(B), which requires issuers with a class of securities registered pursuant to Section 12 of the Exchange Act to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances, among other things, that access to company assets is permitted only in accordance with management's general or specific authorization.

19. As a result of the conduct described above, RRD also violated Exchange Act Rule 13a-15(a), which requires issuers of securities registered pursuant to Section 12 of the Exchange Act, such as RRD, to maintain disclosure controls and procedures designed to ensure that information required to be disclosed by an issuer in reports it files or submits under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms.

RRD's Cooperation and Remedial Efforts

20. In determining to accept the Offer, the Commission considered remedial acts promptly undertaken by Respondent and cooperation afforded the Commission staff. Respondent provided assistance to Commission staff and took other steps, including:

- reporting the 2021 Ransomware Intrusion to the staff prior to Respondent's first EDGAR filing disclosing the 2021 Ransomware Intrusion;

- voluntarily revising incident response policies and procedures, adopting new cybersecurity technology and controls, updating employee training, and increasing cybersecurity personnel;

- providing staff with detailed explanations and summaries of specific factual issues at all stages of the staff's investigation; and

- promptly following up on several requests from staff without requiring subpoenas, including obtaining information from various employees, providing additional documents, and explaining technical cybersecurity issues.

IV.

In view of the foregoing, the Commission deems it appropriate to impose the sanctions agreed to in Respondent RRD's Offer.

Accordingly it is hereby ORDERED that:

A. Pursuant to Section 21C of the Exchange Act, Respondent RRD cease and desist from committing or causing any violations and any future violations of Exchange Act Section 13(b)(2)(B) and Rule 13a-15(a).

B. Respondent RRD shall, within 10 days of the entry of this Order, pay a civil money penalty in the amount of $2.125 million to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Exchange Act Section 21F(g)(3). If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. §3717. Payment must be made in one of the following ways:

(1) Respondent may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

(2) Respondent may make direct payment from a bank account via Pay.gov through the SEC website at http://www.sec.gov/about/offices/ofm.htm; or

(3) Respondent may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center
Accounts Receivable Branch
HQ Bldg., Room 181, AMZ-341
6500 South MacArthur Boulevard
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying R.R. Donnelley & Sons Co. as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to David Hirsch,

Chief of the Crypto Assets and Cyber Unit, Division of Enforcement, Securities and Exchange Commission, 100 F St., NE, Washington, DC 20549.

C. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, it shall not argue that it is entitled to, nor shall it benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that it shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

D. Respondent acknowledges that the Commission is not imposing a civil penalty in excess of $2.125 million based upon its cooperation in a Commission investigation or related enforcement action. If at any time following the entry of the Order, the Division of Enforcement ("Division") obtains information indicating that Respondent knowingly provided materially false or misleading information or materials to the Commission, or in a related proceeding, the Division may, at its sole discretion and with prior notice to the Respondent, petition the Commission to reopen this matter and seek an order directing that the Respondent pay an additional civil penalty, Respondent may contest by way of defense in any resulting administrative proceeding whether it knowingly provided materially false or misleading information, but may not: (1) contest the findings in the Order; or (2) assert any defense to liability or remedy, including, but not limited to, any statute of limitations defense.

By the Commission.

Vanessa A. Countryman
Secretary