SEC Enforcement Case Summary
R.R. Donnelley Charged with Cybersecurity Control Violations

On June 18, 2024, R.R. Donnelley & Sons Company (***RRD***), a global provider of business communications and marketing services, agreed to pay over $2.1 million in a settled enforcement action with the Securities and Exchange Commission (***SEC***) for disclosure and internal control failures related to cybersecurity incidents. The case was brought by the SEC's Crypto Assets and Cyber Unit.

According to the SEC order, RDD's IT network regularly stored and transmitted confidential client data and information, including business plans as well as personal identifying and financial information of customers. Over a three-month period in late 2021 and early 2022, RDD's internal intrusion detection systems issued a significant number of alerts, which were reviewed initially by the firm's third-party managed services provider (***MSSP***). After review and analysis, the MSSP would escalate 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. The SEC faulted RDD for not reasonably managing the MSSP's allocation of resources for such activity, given the high volume and complexity of the alerts, failing to audit or confirm the MSSP's process for reviewing and escalating alerts, failing to dedicate sufficient time or resources to manage escalated alerts, and inadequate policies and procedures that 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.

RDD experienced a ransomware intrusion in late 2021 and the MSSP escalated alerts to internal cybersecurity personnel. According to the SEC order, 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. However, RDD did not take the infected instances off the network and failed to promptly conduct an adequate investigation or remedial action to prevent further compromise. The SEC noted that in at least 20 other instances, RDD was alerted to malware being installed or executed on multiple computers, allowing threat actors to utilize deceptive hacking techniques to install encryption software on RDD computers (mostly virtual machines) and exfiltrate significant amounts of data, including personal identification and financial information. Once the firm's Chief Information Security Officer was alerted to such activity, RDD 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 ransomware Intrusion.

The SEC charged RDD with violations under the Securities Exchange Act of 1934 (***Exchange Act***) requiring public issuers 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. The firm was further charged with failing 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.

While RDD was required to pay a significant penalty in the settled action, as noted above, the SEC order noted that the staff considered the firm's cooperation in the investigation and voluntary document production without requiring subpoenas. The SEC further acknowledged remedial actions the firm took, including disclosure of the ransomware intrusion in public filings, voluntarily revising incident response policies and procedures, adopting new cybersecurity technology and controls, updating employee training, and increasing cybersecurity personnel.

Private funds and investment advisers are not subject to the Exchange Act provisions under which this case was brought. However, recent changes for Regulation S-P, proposed cybersecurity risk management rulemaking and regulatory guidance demonstrate that the SEC is similarly concerned that investment advisers adopt, implement, and maintain robust cybersecurity programs and incident response plans.

See Press Release – https://www.sec.gov/newsroom/press-releases/2024-75