VedderPrice

SEC Proposes New Cybersecurity Rules for Investment Advisers and Investment Companies

By Joseph M. Mannon, Jeff VonDruska and Rachel Behar

February 11, 2022

On February 9, 2022, the Securities and Exchange Commission (the SEC) issued proposed rules 206(4)-9 under the Investment Advisers Act of 1940, as amended (Advisers Act) and 38a-2 under the Investment Company Act of 1940 (Investment Company Act) (such rules collectively referred to as the 'cybersecurity risk management rules'), to require investment advisers registered under the Advisers Act (advisers) and registered investment companies under the Investment Company Act (funds) to adopt and implement significant new written cybersecurity policies and procedures. At a high level, the proposed rules would require annual reviews, add new disclosure requirements, and add new SEC and investor reporting requirements, among other requirements.

Highlights of the proposed rules include the following:

Adopting policies and procedures. Advisers and funds would be required to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks. Recognizing that not all advisers and funds have uniform businesses or technology systems, the proposed rules would give advisers and funds flexibility to tailor such policies to the nature and scope of their business and their individual cybersecurity risks. Specifically, the proposed rules would require the policies and procedures to address certain specific areas, including performance of periodic risk assessments, user security and access, information protection, threat and vulnerability management, and incident response and recovery. Importantly, the proposed rules would provide flexibility for advisers and funds to determine the person(s) responsible for implementation and oversight of the policies, in addition to flexibility to outsource certain cybersecurity responsibilities.

Annual review of policies and procedures. Advisers and funds would be required to, at least annually, review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether they reflect changes in cybersecurity risk over the time period covered by the review, and prepare a written report. At a minimum, the report would describe the annual review, assessment and any control tests performed, document any cybersecurity incidents, and discuss any material changes to the policies and procedures.

Fund board oversight. Proposed rule 38a-2 would require that a fund's board of directors initially approve its policies, written reports on cybersecurity incidents and material changes to policies that would be required to be prepared at least annually.

New recordkeeping requirements. Under the proposed rules, advisers and funds would be subject to enhanced recordkeeping requirements, including, among other items, annual review reports and supporting records, reports of any significant fund cybersecurity incidents and supporting documentation, and records documenting the cybersecurity risk assessment, each from within the preceding five years.

Cybersecurity-related disclosures. The proposed rules would require disclosure of certain cybersecurity risks and incidents to current and prospective investors and clients, including through updates to an adviser's Form ADV Part 2A, a new proposed section of Form ADV for advisers and a fund's registration statements, as applicable.

The proposed rules are subject to change following the public comment period and further review by the SEC.

If you have any questions regarding the topics discussed in this article, please contact **Joseph M. Mannon** at +1 (312) 609 7883, **Jeff VonDruska** at +1 (312) 609 7563, **Rachel Behar** at +1 (212) 407 7641 or any Vedder Price attorney with whom you have worked.