PUBLICATION

SEC Proposal: New Cybersecurity Risk Management Rules for Investment Advisers and Funds

Authors: Alisa L. Chestler
February 16, 2022

In a show of continued emphasis on cybersecurity enforcement from U.S. government agencies in the wake of the Biden Administration's Executive Order on Improving the Nation's Cybersecurity (Exec. Order No. 14028, May 12, 2021), on February 9, 2022, the Securities and Exchange Commission (SEC) issued proposed rules 206(4)-9 under the Investment Advisers Act of 1940 (Advisers Act) and 38a-2 under the Investment Company Act of 1940 (Investment Company Act), aimed at enhancing the cybersecurity policies and procedures, reviews, and reporting and disclosure requirements of registered investment advisers (advisers) and investment companies (funds).

As currently drafted, the proposed rules include the following key requirements:

Maintenance of Cybersecurity Policies and Procedures

The proposed rules would require advisers and funds to adopt and implement written policies and procedures reasonably designed to address cybersecurity risks. In order to address risks to advisory clients and fund investors, these policies and procedures would be required to address:

1. User security and access,
2. Information protection,
3. Risk assessments,
4. Threats and vulnerability management, and
5. Incident response and recovery.

Advisers and funds would further be required to review and assess the efficacy of their policies and procedures annually, including a report on the assessments performed and any material changes to the policies and procedures.

Disclosure of Cybersecurity Risks and Incidents

Through amended forms for advisers (Form ADV Part 2A) and funds (Forms N-1A, N-2, N-3, N-4, N-6, N-8B-2, and S-6), the proposed rules would require disclosure of cybersecurity risks and incidents to current and prospective clients that could materially affect the advisory relationship; including, in the case of funds, a requirement to disclose cybersecurity incidents that have occurred in the fund's past two fiscal years.

Reporting of Cybersecurity Incidents

The proposed rules would require advisers to report significant cybersecurity incidents to the SEC, including on behalf of a fund, by submitting a newly proposed Form ADV-C within 48 hours of discovery of the incident. A "significant cybersecurity incident" in this context includes an isolated or group of related cybersecurity incidents that significantly disrupts or degrades the adviser's or fund's ability to maintain critical operations, or leads to the unauthorized access or use of adviser or fund information, where the unauthorized access or use of such information results in, in the case of an adviser incident: (1) substantial harm to the adviser; or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed, or, in the case of a fund incident: substantial harm to the fund or to an investor whose information was accessed.

Recordkeeping

Under the proposed rules, advisers and funds would be required to maintain, for a period of five years:

6. Copies of cybersecurity policies and procedures,
7. Copies of annual reviews thereof,
8. Documentation related to such annual reviews,
9. Regulatory filings related to cybersecurity incidents,
10. Documentation of cybersecurity incidents, and
11. Cybersecurity risk assessments.

Oversight by Fund Board

The proposed rules would require particular cybersecurity oversight activities to be performed by a fund's board, including a requirement to approve the fund's initial cybersecurity policies and procedures, as well as a requirement to review the annual report reviewing such policies and procedures.

Next Steps

With the growing threat of malicious cyber-actors who pose risk of harm to both advisory clients and fund investors, the SEC has proposed these more direct cybersecurity requirements with an aim of supporting the agency's goals of protecting investors and maintaining orderly markets. Although a final rule may vary from the current proposed rules, advisers and funds should be prepared to review their current cybersecurity practices and consider how they will implement stricter policy, review, and reporting requirements in the near future. Likewise, in evaluating confidence in any new or existing investment relationship, advisory clients and fund investors should consider how such investment managers are acting to protect them against increasing technological risks in the market. These proposed rules may be the first of several cybersecurity requirements for entities subject to SEC regulation.

The proposed rules are currently open to public comment through the later of April 11, 2022 or 30 days following publication of the proposed regulations in the Federal Register.

For more information contact Alisa Chestler or your Baker Donelson Data Protection, Privacy and Cybersecurity attorney.