faegre drinker

February 15, 2022

SEC Proposes New Cybersecurity Risk Management Rules for Registered Investment Advisers, Registered Investment Companies and Business Development Companies

Authors: David L. Williams, Walé Y. Oriola, Jeremiah Posedel, Heaven L. Chandler

On February 9, 2022, the U.S. Securities and Exchange Commission (SEC) voted to propose cybersecurity rules applicable to investment advisers and registered investment companies, including business development companies. If adopted, the proposed rules — Rule 206(4)-9 under the Investment Advisers Act of 1940, as amended and Rule 38a-2 under the Investment Company Act of 1940, as amended — would require investment advisers and funds to implement written policies and procedures to address cybersecurity risks, and create new reporting, disclosure and record keeping obligations.

Cybersecurity Policies and Procedures

Under the proposed rules, advisers and funds will be required to adopt cybersecurity policies and procedures that are tailored to the nature and scope of their business and reasonably designed to address cybersecurity risks. Speaking at the February 9, 2022 open meeting, Thomas Strumpf from the Division of Investment Management outlined the following general elements that advisers and funds would be required to address in their cybersecurity policies and procedures:

1. Risk assessment of the cybersecurity risks associated with an adviser's or fund's information systems and the information processed by such systems, including the risks associated with service providers that process such information
2. User security controls that limit user related risks while also limiting unauthorized access and use of personal information
3. Information monitoring protection, including performing periodic assessments of their information systems and the information that resides on the systems

4. Threat and vulnerability protections to detect, mitigate and mediate information and system breaches
5. Cybersecurity incident response measures to detect, respond and recover from cyberattacks

Review and Approval Requirements

The proposed rules would mandate the review and approval of the cybersecurity policies and procedures by advisers, funds and their board of directors. To fulfill their review obligations, advisers and funds would be required to conduct an annual review of the cybersecurity polices and procedures and produce a written report summarizing the findings of the review at least once a year. This annual review would need to include an assessment of the design and effectiveness of the cybersecurity procedures, including if they reflect changes in cybersecurity risks over time.

The proposed rules would also require a fund's board of directors, including a majority of its independent directors, initially to approve the fund's cybersecurity policies and procedures, as well as to review the written report on cybersecurity incidents and material changes to the fund's cybersecurity policies and procedures that, as described above, would be required to be prepared at least annually.

Cybersecurity Reporting and Disclosure Requirements

The proposed rules would require new reporting and disclosure requirements for advisers following a cybersecurity incident. Advisers would be required to confidentially report significant cybersecurity incidents on new Form ADV-C within 48 hours of concluding that a significant cybersecurity incident has occurred or is occurring. The rules define a "significant cybersecurity incident" as a single cyber incident or a combination of cyber incidents that significantly disrupt or degrade the adviser's ability, or the ability of a fund or private fund client of the adviser, to maintain critical operations. A "significant cybersecurity incident" also occurs when sustained harm is done to the adviser, client or an investor in a private fund through the use of unauthorized access to the adviser's information. The SEC believes this confidential reporting step will allow the commission and its staff to understand the nature and extent of the incident, review the response effort and evaluate the potential systematic risk to the financial markets as a whole.

The proposed rules would also amend Form ADV Part 2A to require advisers to disclose cybersecurity risks and incidents to advisory clients and prospective clients. Registered funds would be required to disclose in their registration statement any significant cybersecurity incidents that have occurred in the last two fiscal years. The SEC believes the disclosure requirements will enhance investor protections and allow investors to make informed decisions.

Book and Recordkeeping Requirements

Finally, the proposed rules would require advisers and funds to keep cybersecurity related books and records. Advisers and funds would be required to maintain, for five years, documentation of:

1. Cybersecurity policies and procedures
2. Annual reviews thereof
3. Documentation related to the annual reviews
4. Cybersecurity incidents
5. Regulatory filings related to cybersecurity incidents
6. Cybersecurity risk assessments

Call for Public Comments

The public comment period will be open for 60 days following publication of the proposing release on the SEC's website – until April 11, 2022 – or 30 days following publication of the proposing release in the Federal Register, whichever period is longer.

Conclusion

The proposed rules would incorporate existing SEC staff guidance on cybersecurity policies and procedures and also create significant reporting and disclosure requirements relating to cybersecurity incidents. Additionally, the proposed rules would establish formalized oversight responsibilities for fund boards. In the proposed rule release, the SEC directs several questions to the investment adviser and fund industry relating to each element of the rule proposal as it looks to finalize the rules. Given the SEC’s ongoing focus on cybersecurity enforcement, it is likely not a matter of if the proposed rules will be adopted, but how the details of the proposed rules will be revised based on industry comments.

MEET THE AUTHORS

David L. Williams

Partner

+1 312 569 1107
Chicago
david.williams@faegredrinker.com

Walé Y. Oriola

Counsel

+1 202 230 5076
Washington, D.C.
wale.oriola@faegredrinker.com

Jeremiah Posedel

Partner

+1 312 569 1504
Chicago
jeremiah.posedel@faegredrinker.com

Heaven L. Chandler

Associate

+1 312 569 1137
Chicago
heaven.chandler@faegredrinker.com

Services and Industries

Corporate

Investment Management

Government & Regulatory Affairs