

SEC Plants New Cybersecurity Regulations; Time Will Tell What Will Bloom

February 15, 2022

It's planting season for the SEC, and among the seedlings is File Number S7-04-22, a proposed cybersecurity rule intended to increase regulation of advisers' and investment companies' cybersecurity preparedness. As currently drafted, the proposed rule would significantly increase the cybersecurity obligations of SEC-registered investment advisers and companies, including SEC-registered separate accounts of insurance companies.

Although some investment companies and advisers have considered cybersecurity risks as part of their fiduciary obligations and/or implemented written policies and procedures as part of their 17 CFR 270.38a-1, 17 CFR 275(6)-7, Regulation S-P, or Regulation S-ID compliance, the new regulations require a more specific, frequently reviewed, and documented program. The proposed rule would require:

- **Written cybersecurity policies and procedures** reasonably designed to address cybersecurity risks and tailored to a business's operations, including:
 - **Written risk assessments** that categorize and prioritize cybersecurity risks based on specific factors;
 - **Controls designed to minimize user-related risks and prevent unauthorized access**, including specific policies and procedures;
 - **Monitoring and periodic assessments of information systems** and the information that resides therein, including considering specific criteria; and
 - **Threat and vulnerability management**, including detecting, mitigating, and remediating cybersecurity threats and vulnerabilities, including policies and procedures designed to ensure particular elements.

- **At least annual, review of, and a written report** regarding, the effectiveness of those cybersecurity policies and procedures and changes to the threat landscape. The written report must “at a minimum”:
 - Describe the review, assessment, and any control tests performed;
 - Explain the results thereof;
 - Document any cybersecurity incident that occurred since the date of the last report; and
 - Discuss any material changes to the policies and procedures since the date of the last report.
- **Board of directors approval** of the cybersecurity policies and procedures and its annual written report. As with 38a-1 reports, the proposal contemplates that if the investment company is an insurance company separate account or other unit investment trust, the report would be approved by the company’s depositor or principal underwriter;
- **Additional disclosures** to current and prospective advisory clients and investment company securityholders regarding cybersecurity risks and incidents, including amendments to Forms ADV, N-1A, N-2, N-3, N-4, N-6, N-8B-2, and S-6;
- Prompt, but in no event more than 48 hours after having a reasonable basis to conclude a significant incident has occurred, **confidential reporting of “significant cybersecurity incidents affecting the adviser, or its investment company or private fund clients, to the [SEC],”** using Form ADV-C, **and amendments to previously filed forms** within the same timeframe as new material information is discovered;
- Prompt **delivery of material changes** to ADV cybersecurity disclosures **to all of an adviser’s customers**;
- **Public disclosure of significant cybersecurity incidents** from the last two fiscal years **on brochures and registration statements**;
- **Structured interactive data requirements** for Inline XBRL tagging of significant cybersecurity incidents that are disclosed in investment companies’ registration statements; and
- **Other new record-keeping obligations** designed to improve the availability of cybersecurity-related information and facilitate the SEC’s inspection and enforcement capabilities.

The SEC is accepting comments on its proposed new blooms. The comment period will close on the later of April 11, 2022, or 30 days from when published in the Federal Register.

Authored By



Patricia M. Carreiro



Thomas C. Lauerman

Related Practices

[Cybersecurity and Privacy](#)

[Financial Services Regulatory](#)

[Securities Transactions and Compliance](#)

Related Industries

[Securities & Investment Companies](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.