Proskauer

SEC Proposes Cybersecurity Rule for Registered Funds and Investment Advisers

April 28, 2022

Final comments were due last week to the Securities and Exchange Commission (SEC)'s proposed cybersecurity risk management rules for registered investment advisers, registered investment companies and business development companies (registered funds), as well as various amendments to existing rules governing investment adviser and registered fund disclosures. The main focus of the 200 plus page proposed rule is to strengthen existing requirements and foster upgrades to the cybersecurity risk management practices of registered funds and advisers. The vote was 3-1.[1] Cybersecurity has been front of mind for the SEC in recent years, having issued updated guidance on public company cybersecurity disclosures in 2018 and risk alerts in 2020 on credential stuffing and ransomware attacks.

As outlined in the accompanying Cybersecurity Risk Management Fact Sheet, the proposed rule would affect financial sector registrants' cybersecurity practices in a number of key ways, by **REQUIRING:**

- Registered advisers and funds to implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks, including risks of using interconnected systems and networks directly and through IT vendors;
- Registered advisers and funds to memorialize and maintain various recordkeeping obligations surrounding cybersecurity programs and the occurrence of cybersecurity incidents;
- Registered advisers to disclose cybersecurity risks and incidents to the adviser's clients and prospective clients; funds to provide prospective and current investors with cybersecurity-related disclosures;
- Registered advisers to report significant cybersecurity incidents to the SEC (including on behalf of a fund or private fund client); and
- Registered fund boards to undertake additional oversight of a cybersecurity risk management program.

The proposed new rule on cybersecurity risk management and recordkeeping requirements would be promulgated pursuant to the Investment Advisers Act of 1940 ("Advisers Act") and the Investment Company Act of 1940 ("Investment Company Act"), both of which already indirectly require registered advisers and funds to consider certain cybersecurity risks when developing policies and procedures. In addition, the new proposed rule would make additional amendments to various cybersecurity incident disclosure forms and require new timely breach disclosures to the Commission.

Given the sophistication of today's cyber threat actors and organized ransomware groups, the vast majority of financial institutions, including registered advisers and funds have in place some cybersecurity protections and technical measures under existing regulatory frameworks. However, if the SEC's proposed rule is approved, such entities would be obligated to take new, affirmative steps that would undoubtedly add to their compliance load. For example, registered advisers and funds would be required to review the design and efficacy of their cybersecurity policies and procedures *annually* and prepare a *written* report. Moreover, registered funds' board of directors would be tasked with approving cybersecurity policies and procedures, reviewing the annual cybersecurity program report, and taking oversight and accountability for the program.

Below, we will highlight some of the most salient aspects of the SEC's new proposed rule.

Cybersecurity Risk Management Rules

The SEC is proposing that under rules 206(4)-9 under the Advisers Act and 38a-2 under the Investment Company Act, all registered advisers and funds must "adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks."

Given the evolving nature of threats, the SEC believes that the proposed cybersecurity rule would be flexible and covered entities would be able to tailor cybersecurity programs to the nature of their business operations, taking into account their complexity and the changing cybersecurity threats, or whether compliance would come from in-house personnel with appropriate expertise or the retention of a third party cybersecurity risk management service.

The proposed rule touches on some important aspects of a cybersecurity program:

- *Risk assessment*: The proposed rule would require registered advisers and funds periodically to assess and draft*written* risk assessments of the particular threats (and potential ramifications of a significant cyberattack) to their systems, all based on an inventory of the network and its stored data and the presence of service providers that are permitted access to the network (and what cyber risks might be associated with these service providers). Such a program, according to the proposed rule, should be "reasonably designed to ensure its operational capability, including resiliency and capacity of information systems," in the face of a cyberattack. Given the evolving nature of threats, the proposed rule states that advisers and funds should reassess risks "as they arise" in order to prompt internal changes.
- *User security and access*: The proposed rule would require controls designed to minimize user-related risks and prevent unauthorized access to the network by mandating policies that echo cybersecurity protections already practiced by many companies (e.g., robust user authentication procedures and employee information access practices akin to the "principle of least privilege" (including protections that take into account the realities of remote working).
- *Information protection*. Registered funds and advisers would be required to assess the sensitivity of data on its network and thereafter monitor IT systems to identify suspicious activity (including the regular testing of systems, including penetration tests). Such obligations, which undoubtedly are already firmly in place at covered entities, would also require certain third party vendor security oversight practices.
- *Threat and Vulnerability Management*. The proposed cybersecurity risk management rule would require registered advisers and funds to detect, mitigate, and remediate cybersecurity threats and vulnerabilities with respect to adviser or fund information and systems through ongoing monitoring of systems and industry or government cyber threat information.
- *Cybersecurity Incident Response*. The proposed cybersecurity risk management rule would require registered advisers and funds to have measures to detect, respond to, and recover from a cybersecurity incident; such entities would thus be able to continue to provide services to their clients and investors when facing cyber-related disruptions.

Reporting of Significant Cybersecurity Incidents to the SEC

The SEC is proposing a new rule requirement to report "significant cybersecurity incidents" confidentially to the Commission on proposed Form ADV-C "promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident had occurred or is occurring." Notably, this obligation would require registered advisers to report significant cybersecurity incidents to the Commission, *including* on behalf of a registered fund, or a private fund client that "experiences a significant cybersecurity incident." Additionally, the proposed rule would also require registered advisers to amend any previously filed Form ADV-C promptly, "but in no event more than 48 hours, after information reported on the form becomes materially inaccurate; if new material information about a previously reported incident is discovered; and after resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident." This timeline for breach reporting to the SEC under the propose rule would be one of the strictest in the industry when compared with other reporting regimes.[2]

Importantly, the proposed rule would define a "significant adviser cybersecurity incident" as:

> "A cybersecurity incident, or a group of related incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in:

1. substantial harm to the adviser,[3] or
2. substantial harm to a client, or an investor in a private fund, whose information was accessed."[4]

In addition to the above notification requirements, an adviser would also have to report "significant fund cybersecurity incidents" on Form ADV-C for its registered fund clients. Similar to a significant adviser cybersecurity incident, a "significant fund cybersecurity incident" has two prongs:

1. significantly disrupts or degrades the fund's ability to maintain critical operations, or

2. leads to the unauthorized access or use of fund information, which results in substantial harm to the fund, or to the investor whose information was accessed. [5]

In all, according to the proposed rule, a registered adviser would have to report within 48 hours after having a reasonable basis to conclude that any significant adviser or fund cybersecurity incident has occurred or is occurring with respect to itself or any of its clients that are covered clients.

Annual Review

The proposed rule would require registered advisers and funds to review their cybersecurity policies and procedures, at minimum, annually and produce a written report detailing security assessments, documenting security incidents and expounding on any material changes to policies and procedures since the last report. The text of the proposed rule hints at the expectation that security experts might handle the bulk of report preparation, but the SEC advises that personnel overseeing the cybersecurity program should also provide an organizational perspective.

Registered Fund Board Oversight

Under the proposed rule, the SEC would require a registered fund's board of directors, including a majority of its independent directors, to initially approve the fund's cybersecurity program, as well as to review the annual written report. The proposed rule states that boards should also consider what level of cybersecurity oversight of the fund's service providers is appropriate.

Recordkeeping

The proposed rule would amend both the Advisers Act and Investment Company Act to add additional recordkeeping requirements, namely maintaining five years of cybersecurity policies, annual written cybersecurity reports, risk assessments, breach notification notices, and records documenting "any cybersecurity incidents," including incident response (e.g., incident logs, longer descriptions).

Disclosure of Cybersecurity Risks and Incidents

The SEC is also proposing amendments to certain forms used by advisers and funds to provide a more fulsome disclosure of cybersecurity risks and incidents to their investors and other market participants. The proposed amendments would add a new Item 20 entitled "Cybersecurity Risks and Incidents" to Form ADV's narrative brochure, or Part 2A, a publicly available disclosure about an investment adviser's business practices for clients and prospective clients. Under the amended form, advisers would be required to describe cybersecurity risks that could materially affect the services they offer as well as how they assess, prioritize, and address cybersecurity risks created by the nature and scope of their business.[6] Of particular note, the amended form would require registered advisers to describe any cybersecurity incidents that occurred within the last two fiscal years that have "significantly disrupted or degraded the adviser's ability to maintain critical operations," or that have led to the unauthorized access that resulted in substantial harm to the adviser or its clients. This proposed new reporting requirement would also obligate registered advisers to deliver interim brochure amendments "swiftly" to existing clients in the event of material revisions.

Proposed Amendments to Registered Fund Registration Statements

The proposed rule also would require amendments to registered funds' registration forms that would require a description of any "significant fund cybersecurity incident" that has occurred in its last two fiscal years affecting the registered fund or its service providers. The requirements for disclosure describing the incident would be similar to the information required in new Form ADV-C. Similarly, as registered funds are currently required to disclose "principal risks" of investing in the fund, the new proposed rule would require amendments to a registered fund's prospectus if a fund determines that a cybersecurity risk is a principal risk of investing in the fund. In addition, as stated in the proposed rule, registered funds should generally include in their annual reports to shareholders a discussion of cybersecurity risks and significant fund cybersecurity incidents, to the extent that these were factors that materially affected performance of the fund over the past fiscal year.

---

[1] Commissioner Hester Peirce voted against, seemingly preferring that the Commission should have released detailed guidance to assist the industry with a building resilient system as opposed to "rules that set forth detailed cybersecurity prescriptions could become an easy hook for an enforcement action…"

[2] However, even within other reporting regimes, reporting timeframes are nevertheless typically quite short. Some state breach notification laws, for example, require reporting "without unreasonable delay." Some state financial regulators have issued deadlines closer to the SEC's proposed rule (e.g., the New York State Department of Financial Services requires covered entities to notify the superintendent not later than 72-hours from the determination of a reportable cybersecurity event); this comports with the GDPR's 72 hour breach deadline of notification to the competent supervisory authority. Still, the SEC's proposed reporting timeframe is not the shortest among recent proposals: the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency issued a final rule in November 2021 (effective in April 2022) that established a 36-hour deadline for incident notification for banking organizations and their bank service providers.

[3] The proposed rule describes instances of when "substantial harm" to an adviser results from a cybersecurity incident (e.g., if a breach affects an adviser such that it is "unable to maintain critical operations such as the ability to implement its investment strategy, process or record transactions, or communicate with clients…"). Substantial harm to an adviser as the result of a cybersecurity incident in which adviser information is compromised could include, among other things, significant monetary loss or theft of intellectual property.

[4] Under the proposed rule, a significant adviser cybersecurity incident would also include significant cybersecurity incidents affecting private fund clients of an adviser. As stated, substantial harm to a client or an investor in a private fund as the result of a cybersecurity incident in which adviser information is compromised could include, among other things, "significant monetary loss or the theft of personally identifiable or proprietary information."

[5] In this instance, the proposed rule states that "significant fund cybersecurity incidents" may include attackers interfering with a fund's ability to redeem investors, calculate NAV or otherwise conduct its business, as well as incidents involving "the theft of fund information, such as non-public portfolio holdings, or personally identifiable information of the fund's employees, directors or shareholders."

[6] As defined, a “cybersecurity risk” would be “material” to an adviser’s advisory relationship with its clients if “there is a substantial likelihood that a reasonable client would consider the information important based on the total mix of facts and information.”

Related Professionals

- **Robert H. Sutton**
  Partner