KIRKLAND & ELLIS

Kirkland AIM

SEC Proposes Significant New Cybersecurity Rules for Investment Advisers

14 March 2022

On February 9, 2022, the U.S. Securities and Exchange Commission ("SEC") voted (3-1)[1] to propose new cybersecurity requirements for SEC-registered investment advisers under the Investment Advisers Act of 1940 (the "Advisers Act") and SEC-registered investment companies under the Investment Company Act of 1940 (the "Investment Company Act").[2] The proposed rules follow several cybersecurity alerts, reports and enforcement actions from the SEC over the last several years.[3] While most SEC-registered investment advisers already have adopted and implemented cybersecurity policies and procedures, the proposed rules contain more prescriptive requirements compared to existing SEC cybersecurity guidance and rules related to safeguarding information such as Regulation S-P, and would require most registered advisers to implement enhancements to their cybersecurity programs. The proposed rules would also impose reporting and disclosure obligations relating to cybersecurity incidents and risks. Therefore, advisers will likely need to commit additional resources to cybersecurity and be prepared for greater scrutiny of their cybersecurity practices by the SEC and investors.

If adopted, the proposed rules would require SEC-registered advisers to: (1) adopt and implement written cybersecurity policies and procedures, (2) confidentially report significant cybersecurity incidents to the SEC through a new Form ADV-C; and (3) enhance disclosures to investors related to cybersecurity incidents and risks. Each of these categories is discussed in more detail below.

Policies and Procedures

The SEC's proposal would require SEC-registered advisers to establish cybersecurity policies and procedures that include:

- periodic risk assessments, including the identification of risks related to service providers that receive adviser information[4] or are permitted to access adviser information systems;[5]
- controls designed to minimize user-related risks and prevent unauthorized access to adviser information and adviser information systems (e.g., two-factor authentication);
- monitoring of adviser information systems, and protection of adviser information from unauthorized access or use, including through "data mapping" and procedures for oversight of relevant service providers (i.e., contractual provisions requiring service providers to implement measures to protect adviser information and to notify the adviser of cybersecurity incidents);
- measures to detect, mitigate and remediate cybersecurity threats (e.g., vulnerability assessments, scans and training); and
- measures to detect, respond to, recover from and, if necessary, report cybersecurity incidents.

Advisers would also be required to periodically review, at least annually, the design and effectiveness of their cybersecurity policies and procedures. Additionally, at least annually, advisers must prepare a written report that describes the periodic review and any control tests performed, explains the results of the review, describes any cybersecurity incidents since the last report, and discusses the material changes to the policies and procedures since the last report.

Reporting

The SEC's proposal also requires SEC-registered advisers to report "significant cybersecurity incidents" to the SEC on proposed Form ADV-C. A cybersecurity incident would be considered significant if it: (1) significantly disrupts or degrades the ability of the adviser, or a private fund[6] client of the adviser, to maintain critical operations (e.g., the ability to implement the fund's investment strategy or communicate with clients); or (2) leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: substantial harm to the adviser, or substantial harm to an adviser's client, or an investor in a private fund, whose information was accessed (e.g., significant monetary loss, or theft of intellectual property or personally identifiable information, as applicable). Such reports would be confidential and not publicly available.

Notably, the report about the incident would need to be filed with the SEC promptly, but in no event more than 48 hours after having a reasonable basis to conclude that

an incident has occurred or is occurring. The proposed rules emphasize that advisers should not wait until after definitively concluding that an incident has occurred or is occurring. The proposed rules would also require an amendment to any previously filed Form ADV-C for certain material developments regarding a "significant cybersecurity incident," as well as upon the resolution of such incident.

Disclosures

The proposed rules also would amend Form ADV Part 2A, which is publicly available, to include a new section requiring disclosure, in plain English, regarding cybersecurity risks that could materially affect the advisory services provided by the adviser, and how the adviser assesses, prioritizes and addresses cybersecurity risks created by the nature and scope of their business. The proposed amendments would also require 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 or use of adviser information, resulting in substantial harm to the adviser or its clients.[7] The disclosure would need to be fairly detailed, including the identity of the entity or entities affected, when the incidents were discovered and whether they are ongoing, whether any data was stolen, altered or accessed or used for any other unauthorized purpose, the effect of the incident on the adviser's operations, and whether the adviser, or its service provider(s) has remediated or is currently remediating the incident. Noting that "time is of the essence" during a cybersecurity incident, the proposed rules would require an adviser to deliver interim amendments to Form ADV Part 2A to clients promptly upon adding disclosure of a cybersecurity incident (or materially revising a disclosure regarding a previously disclosed incident).[8]

* * * *

Advisers should begin considering the potential application of the proposed rules to their current practices, which may require augmentation of internal and external resources.[9] Given the SEC's focus on cybersecurity over the last several years, the proposed rules are likely to be adopted in a form that is generally consistent with the proposal.

A public comment period will remain open for the SEC's proposed rules until April 11, 2022, which is a relatively short comment period given the extensive nature of this proposal and the SEC's other recent rule proposals.

Please contact the Kirkland regulatory attorneys with whom you regularly work if you have questions regarding these proposals.

---

1. Commissioner Peirce, appointed by President Trump, issued a dissenting statement regarding the proposed rules. ↩

2. This alert focuses on the rule proposals applicable to SEC-registered advisers, although the substantive provisions of the rule proposals applicable to registered investment companies (e.g., publicly offered mutual funds) are substantially similar. The SEC fact sheet summarizing the full proposal is available through this link. ↩

3. *See*, e.g., OCIE Issues Observations on Cybersecurity and Resiliency; Supreme Court Refuses to Hear FINRA Pay-to-Play Challenge, *Kirkland AIM* (Feb. 14, 2020); Recent SEC Developments on Examination Deficiencies, Ransomware, Purchasing 144A Securities and the Form 13F Reporting Threshold, *Kirkland AIM* (July 24, 2020); SEC Announces Three Actions Charging Deficient Cybersecurity Procedures, *SEC Press Release* (Aug. 30, 2021). The SEC also shares cybersecurity resources and guidance on its "Spotlight on Cybersecurity" website. ↩

4. "Adviser information" is proposed to be defined as "any electronic information related to the adviser's business, including personal information, received, maintained, created or processed by the adviser." ↩

5. "Adviser information systems" is proposed to be defined as "information resources owned or used by the adviser, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of adviser information to maintain or support the adviser's operations." ↩

6. A "private fund" is an issuer qualifying for the exemption from investment company status under Investment Company Act Section 3(c)(1) — 100-or-fewer beneficial owners — or 3(c)(7) — solely qualified purchaser owners. The proposed rule would not appear to cover pooled investment vehicles relying on exemptions other than 3(c)(1) or 3(c)(7), such as equity or debt real estate funds relying on the exemptions under Section 3(c)(5)(C) or the Investment Company Act's statutory test; however, the SEC has requested comment on whether advisers to funds that rely on 3(c)(5)(C) should be required to report on significant cybersecurity incidents regarding such funds. ↩

7. This aspect of the proposed rule appears to be particularly ill suited to protecting adviser clients since it would publicly alert hackers to potential target firms. ↩

8. In addition to the requirements discussed herein, the proposed rules separately include amendments to the books and records rule under the Advisers Act that would require advisers to retain records to facilitate the SEC's ability to assess an adviser's compliance with such rules. ↩

9. Unlike SEC-registered funds (e.g., publicly offered mutual funds), the proposed rules would not apply to private funds themselves. In the proposing release, the SEC notes that private funds "may" separately be subject to the Federal Trade Commission's recently amended Standards for Safeguarding Customer Information (the "FTC Rule"). *See* Federal Trade Commission, Standards for Safeguarding Customer Information (Dec. 9, 2021). Similar to the SEC's rule proposals, the FTC Rule generally requires financial institutions (not including registered advisers, but potentially including exempt reporting advisers) to develop, implement and maintain a comprehensive information security program. As the SEC notes in its rule proposal, although the FTC Rule is narrower in scope and generally more prescriptive than the SEC's proposed rules, the FTC Rule is congruent with the requirements of the SEC's proposed rules for cybersecurity policies and procedures and annual reviews. Although the FTC Rule became effective on January 10, 2022, the compliance date for nearly all new requirements under the rule is December 9, 2022. ↩

Authors

Norm Champ, P.C.

Partner / New York

Scott A. Moehrke, P.C.

Partner / Chicago

Michael Chu

Partner / Chicago

Matthew Cohen

Partner / Bay Area – San Francisco / Los Angeles – Century City

Marian Fowler

Partner / Washington, D.C.

Phil Vincent Giglio

Partner / Chicago

Nicholas A. Hemmingsen

Partner / Chicago

Alpa Patel, P.C.

Partner / Chicago

Eric L. Perelman

Partner / New York

Noah Qiao

Partner / New York

Jaime Doninger Schechter

Partner / New York

Christopher J. Scully

Partner / Chicago

Reed T. Schuster

Partner / Chicago

Sunil Shenoi

Partner / Chicago

Ryan P. Swan

Partner / Chicago

Jamie Lynn Walter, P.C.

Partner / Washington, D.C.

Josh Westerholm, P.C.

Partner / Chicago

Related Services

Practices

- Transactional
- Investment Funds

Suggested Reading

- 18 February 2022 Kirkland AIM SEC Proposes Sweeping Rule Changes for Private Fund Advisers (Part 2 of 2)
- 10 February 2022 Kirkland AIM SEC Proposes Sweeping Rule Changes for Private Fund Advisers (Part 1 of 2)
- 04 February 2022 Kirkland AIM SEC Risk Alert Details Additional Private Fund Adviser Examination Deficiencies