Services

Business, Corporate & Securities

Privacy and Data Security

Securities Litigation

SEC Proposes Cybersecurity Risk Management Rules for Investment Advisers

On February 9, 2022, in a long-awaited release, the Securities and Exchange Commission ("SEC") formally proposed new rules related to cybersecurity risk management for Registered Investment Advisers and Funds. Formally titled "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies," the proposed rules[1] will impact and change the way in which Registered Investment Advisers ("RIAs") operate.

The Main Components of the Proposed Rules

The SEC's Fact Sheet on the proposed rules delineate four main areas that the proposed rules would impact. The SEC's proposed rules would:

- Require advisers and funds to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks;
- Require advisers to report significant cybersecurity incidents to the SEC on a proposed Form ADV-C;
- Enhance adviser and fund disclosures related to cybersecurity risks and incidents; and
- Require advisers and funds to maintain, make and retain certain cybersecurity-related books and records.[2]

Proposed Form ADV-C

Perhaps the most interesting provision of the proposed rules is the SEC's requirement for RIAs to report "significant" cybersecurity incidents to the SEC on a new form (Form ADV-C). Under the proposed rules, RIAs must report "significant" cybersecurity incidents within forty-eight (48) hours.[3] Specifically, the proposed rule would "require advisers to report certain information regarding a significant cybersecurity incident in order to allow the [SEC] and its staff to understand the nature and extent of the cybersecurity incident and the adviser's response to the incident."[4]

---

[1] https://www.sec.gov/rules/proposed/2022/33-11028.pdf?utm_medium=email&utm_source=govdelivery

[2] https://www.sec.gov/files/33-11028-fact-sheet.pdf at 1.

[3] https://www.sec.gov/rules/proposed/2022/33-11028.pdf?utm_medium=email&utm_source=govdelivery at 46.

[4] https://www.sec.gov/rules/proposed/2022/33-11028.pdf?utm_medium=email&utm_source=govdelivery at 56.

What does a "significant" cybersecurity event mean? According the proposed rules, a "significant" cybersecurity incident is defined as, "a cybersecurity incident, or a group of related incidents, **that significantly disrupts or degrades** the adviser's ability…**to maintain critical operations, or leads to the unauthorized access or use of advisor information**, where the unauthorized access or use of such information results in: (1) substantial harm to the adviser, or (2) substantial harm to a client… whose information was accessed."[5] The ongoing interpretation of a "significant" cybersecurity event will be important for RIAs to watch and follow, so that they can accurately report their own incidents, while not reporting incidents that are not "significant."

New Form ADV-C[6] would, among other items, require advisers to provide the SEC with the following:

- Substantive information about the nature and scope of the incident being reported, including any actions and planned actions to recover from the incident;
- Whether any data was stolen, altered or accessed or used for any other unauthorized purpose; and
- Whether the significant cybersecurity incident has been disclosed to the adviser's clients and/or to investors.[7]

In the proposed rules, the SEC states that "an adviser may need time to determine the scope and effect of the incident to provide meaningful responses to these questions [on Form ADV-C]." The SEC goes on to state, however, that "advisers should have sufficient information to respond to the proposed questions [on Form ADV-C] by the time the filing is due to the Commission. Advisers should only share information about what is known at the time of filing."[8] The proposed rules presume that the adviser has sufficient systems in place, as well as IT experts and lawyers, to evaluate and advise whether a potential incident is a reportable incident. The proposed rules will force advisers to preplan for such a scenario and have competent professionals at the ready should the advisor be subject to such a cyber incident.

Cybersecurity Insurance

The proposed rules also discuss cybersecurity insurance and the proposed requirements of RIAs to notify the SEC and the RIAs insurer about a significant cybersecurity incident. The proposed rules note that an RIA "may also see an increase in its insurance premiums" because of a cybersecurity incident.[9]

For example, Form ADV-C would "require the adviser to disclose [to the SEC] whether the cybersecurity incident is covered under a cybersecurity insurance policy."[10] Form ADV-C also requires the RIA to inform the SEC whether or not the RIA has already contacted the insurance company about the "significant cybersecurity incident."[11]

---

[5] https://www.sec.gov/rules/proposed/2022/33-11028.pdf?utm_medium=email&utm_source=govdelivery at 47.

[6] https://www.sec.gov/rules/proposed/2022/33-11028.pdf?utm_medium=email&utm_source=govdelivery at 239-43.

[7] https://www.sec.gov/rules/proposed/2022/33-11028.pdf?utm_medium=email&utm_source=govdelivery at 57.

[8] https://www.sec.gov/rules/proposed/2022/33-11028.pdf?utm_medium=email&utm_source=govdelivery at 58.

[9] https://www.sec.gov/rules/proposed/2022/33-11028.pdf?utm_medium=email&utm_source=govdelivery at 7.

[10] https://www.sec.gov/rules/proposed/2022/33-11028.pdf?utm_medium=email&utm_source=govdelivery at 58.

[11] https://www.sec.gov/rules/proposed/2022/33-11028.pdf?utm_medium=email&utm_source=govdelivery at 243.

Contacts

Jon Breyer
Minneapolis
612.334.5057
jon.breyer@kutakrock.com

Andrew Shedlock
Minneapolis
612.334.5022
andrew.shedlock@kutakrock.com

The SEC requests this information because information about insurance "would assist the [SEC] in understanding the potential effect that incident could have on an adviser's clients."[12] The SEC also notes that information regarding an RIA's cybersecurity insurance would be "helpful in evaluating the adviser's response to the incident given that cybersecurity insurance may require an adviser to take certain actions during and after a cybersecurity incident."[13]

In light of the proposed rules, RIAs should review existing cybersecurity insurance policies and evaluate whether their insurance policies are sufficient to cover a cybersecurity incident.

Comments to the SEC About the Proposed Rules

What can you do to make your voice heard? Submit comments to the SEC within 30 days. You can do so by either using the SEC's internet comment form or by sending an email to rule-comments@sec.gov, while making sure to include File Number S7-04-22 on the subject line. We are also prepared to submit comments on your behalf and pool comments of our similarly situated clients to maximize the impact of our clients' concerns. The proposed rules are not final and have not taken affect. RIAs and other industry members have the opportunity to make their voices heard before the rules become final. Please contact us if you would like to submit a comment or join in the comments of other impacted RIAs.

Additional Information

This Client Alert is not intended to be legal advice or a comprehensive analysis of the proposed rules, but rather an overview of a few provisions of the proposed rules. For further information about how we can advise you with respect to these proposed rules, please contact your Kutak Rock attorney or one of the authors listed on the left. You may also visit us at www.KutakRock.com.

[12] https://www.sec.gov/rules/proposed/2022/33-11028.pdf?utm_medium=email&utm_source=govdelivery at 58.

[13] https://www.sec.gov/rules/proposed/2022/33-11028.pdf?utm_medium=email&utm_source=govdelivery at 58.