Milbank Insights

Litigation & Arbitration Group

SEC Proposes Unprecedented Cybersecurity Rules for Investment Advisers and Funds

February 11, 2022

Contact

Adam Fee, Partner
+1 212.530.4401
afee@milbank.com

Antonia M. Apps, Partner
+1 212.530.5357
aapps@milbank.com

George S. Canellos, Partner
+1 212.530.5792
gcanellos@milbank.com

Sean M. Murphy, Partner
+1 212.530.5688
smurphy@milbank.com

Joel Harrison, Partner
+44 20.7615.3051
jharrison@milbank.com

Matthew Laroche, Special Counsel
+1 212.530.5514
mlaroche@milbank.com

On February 9, 2022, the SEC voted to propose rules mandating sweeping cybersecurity measures for registered advisers and funds.[1] The proposal reflects the first SEC rules specifically addressing cybersecurity programs and reporting.

Most notably, the rules would impose a rapid reporting requirement when advisers face serious cyberattacks. Advisers would have to report any "significant cybersecurity incident" within 48 hours of its discovery by confidentially filing a proposed new Form ADV-C.

The reporting requirement would be triggered if (1) a cyberattack "significantly disrupts or degrades" the ability of an adviser or its private fund clients to "maintain critical operations," or (2) the attack results in unauthorized access to "adviser information" or "fund information" resulting in "substantial harm" to the adviser, its clients, a fund, or investors. The proposed rule offers specific examples of "significant cybersecurity incidents," including a malware attack that shuts down an adviser's "websites or email functions" or a system breach that impedes a fund's ability to "conduct its business" or results in the "theft of fund information."

The 48-hour clock begins to tick as soon as an adviser has a "reasonable basis to conclude" that a significant incident has or is occurring. Certainty is not the standard. The proposed rules make clear that advisers must not wait until they "definitively conclude[] that an incident has occurred or is occurring."

Beyond the 48-hour reporting requirement, the proposed rules would impose other novel cybersecurity requirements on advisers and funds, including:

- Form ADV would be amended to require advisers to publicly disclose detailed information concerning significant cybersecurity incidents that occurred within the prior two years and any "material" cybersecurity risks, and funds would be required to make similar disclosures to their prospective and current investors.

1 The SEC simultaneously published the Proposed Rules (Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies), along with a fact sheet (Cybersecurity Risk Management Fact Sheet) and press release (Press Release SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds).

- Advisers and funds would be required to adopt and implement cybersecurity policies and procedures containing risk assessments, controls addressing user-related risks and unauthorized access to information and systems, cybersecurity incident response and recovery, and other elements.
- New recordkeeping requirements would compel advisers and funds to maintain records relating to cybersecurity incident responses and related materials.

If adopted, these proposed rules would reflect the most detailed and onerous cybersecurity-related requirements imposed on advisers and funds at the national level. They would require many covered entities to overhaul their procedures for managing and addressing cybersecurity risks, and dramatically increase the prospect of SEC enforcement actions for noncompliance with the proposed rules.

While many viewed the pronouncement of cyber-specific rules as long overdue, this proposal reflects an especially aggressive approach by the SEC. We anticipate significant industry pushback on the breadth of the proposed rules during the public comment period, which will be the longer of either 60 days from February 9, 2022, or 30 days after publication of the proposal in the Federal Register.

Litigation & Arbitration Group Contacts

New York | 55 Hudson Yards, New York, NY 10001-2163

Antonia M. Apps	aapps@milbank.com	+1 212.530.5357
George S. Canellos	gcanellos@milbank.com	+1 212.530.5792
Adam Fee	afee@milbank.com	+1 212.530.4401
Sean M. Murphy	smurphy@milbank.com	+1 212.530.5688
Matthew Laroche	mlaroche@milbank.com	+1 212.530.5514

Technology Practice

London | 100 Liverpool Street, London, UK EC2M 2AT

Joel Harrison	jharrison@milbank.com	+44 20.7615.3051

Please feel free to discuss any aspects of this Client Alert with your regular Milbank contacts or any member of our Litigation & Arbitration Group.

This Client Alert is a source of general information for clients and friends of Milbank LLP. Its content should not be construed as legal advice, and readers should not act upon the information in this Client Alert without consulting counsel.