April 11, 2022

VIA ELECTRONIC SUBMISSION

Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549-1090

Re: 48-Hour Cybersecurity Incident Reporting Requirement under Proposed Rule 17 CFR 275.204-6, Pursuant to the Advisers Act (SEC Release No. IA-5956; File No. S7-04-22 (February 9, 2022))

Dear Ms. Countryman:

The American Investment Council (the "AIC") appreciates the opportunity to submit this letter to the Securities and Exchange Commission (the "SEC") on the proposal (the "Proposed Rule") to adopt Rule 204-6 pursuant to the Investment Advisers Act of 1940 (the "Advisers Act").[1]

The AIC is an advocacy, communications, and research organization established to advance access to capital, job creation, retirement security, innovation, and economic growth by promoting responsible long-term investment. In this effort, the AIC develops, analyzes, and distributes information about the private equity and private credit industries and their contributions to the U.S. and global economy. Established in 2007, and formerly known as the Private Equity Growth Capital Council, the AIC is based in Washington, D.C. The AIC's members are the world's leading private equity and private credit firms, united by their commitment to growing and strengthening the businesses in which they invest.[2]

The AIC has supported and continues to support transparency as it relates to cybersecurity risks, and appreciates the opportunity to provide comments on potential challenges that the

[1] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, SEC Release No. IA-5956; File No. S7-04-22 (Feb. 9, 2022) (the "Proposing Release").

[2] For further information about the AIC and its members, please visit our website at http://www.investmentcouncil.org.

implementation of the Proposed Rule would have on private fund advisers registered under the Advisers Act ("Private Fund Advisers").

This letter contains three sections. The first section summarizes the Proposed Rule's applicability to Private Fund Advisers, the second section highlights some of the key challenges associated with the Proposed Rule, and the third section proposes alternative solutions that would further the SEC's goals while alleviating some of the burden on Private Fund Advisers.

I. The Proposed Rule's Applicability to Private Fund Advisers

The Proposed Rule would require Private Fund Advisers, "including on behalf of a client that is a registered investment company or business development company, or a private fund" (collectively, "Covered Clients"), to report any significant cybersecurity incidents, which are defined as any event that (1) "significantly disrupts or degrades the adviser's" or private fund client's "ability to maintain critical operations" or (2) "leads to the unauthorized access or use of adviser information" resulting in substantial harm to the Private Fund Adviser, or substantial harm to a client, or an investor in a private fund, whose information was accessed.[3]

Private Fund Advisers, on behalf of themselves and their Covered Clients, must report to the SEC within 48 hours from when they have a reasonable basis to believe such an incident has occurred. Private Fund Advisers would notify the SEC using a new Form ADV-C, which would include a detailed description of the nature and scope of the incident and any disclosures about it. Private Fund Advisers will be expected to update any previously submitted Forms ADV-C when there has been a material change in facts involving a previously disclosed cybersecurity incident. The Proposed Rule states that submitted Forms ADV-C will remain confidential and not be disclosed to the general public.[4]

[3] Proposing Release at 13536.

[4] Private Fund Advisers that are affiliated with public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934 may additionally be bound by the separate notification requirements of Proposed Item 1.05 to Form 8-K, which would require such public companies to disclose information about a cybersecurity incident within four business days of a determination that the incident was material. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, SEC Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22 (Mar. 9, 2022)).

II. Why the Proposed Rule Is Not Optimal for Meeting the SEC's Objectives.

The stated purpose of the incident reporting provisions of the Proposed Rule is to "help [the SEC] in [its] efforts to protect investors in connection with cybersecurity incidents by providing prompt notice of these incidents . . . [and] allow the Commission and its staff to understand the nature and extent of a particular cybersecurity incident and the firm's response to the incident."[5]

Under the Proposed Rule, the deadline for notification of a significant cybersecurity incident is 48 hours from when a Private Fund Adviser has a reasonable basis to believe that such an incident has occurred or is occurring. In many cases, however, very little is known about a cybersecurity incident in the first 48 hours, and what is known is often incorrect or incomplete. Moreover, the "substantial harm" standard, as drafted, is too vague to elicit meaningful reporting. Private Fund Advisers will likely over-report incidents out of concern that the SEC may second-guess decisions not to report. Specifically, under the current proposal, many Private Fund Advisers will likely choose to provide placeholder notifications, which include little or no details, to the SEC about cybersecurity events, regardless of the import or actual harm of these events. Private Fund Advisers will be concerned that waiting to determine whether the incident meets the Proposed Rule's notification requirements would cause them to violate the 48-hour requirement, thus placing them in jeopardy of examination or enforcement scrutiny for noncompliance with this deadline. As such, to avoid that risk, many Private Fund Advisers will choose to notify the SEC within 48 hours of discovery of any cybersecurity incident in order to ensure compliance with the notification deadline regardless of the quality of the disclosure or the significance of the cybersecurity incident.

Accordingly, having a 48-hour notification deadline will likely mean that the SEC will be inundated with numerous placeholder notifications that are of little value because they either contain no real information, or information that is likely to change swiftly as the Private Fund Adviser continues to investigate the incident. This flood of notices will make it very difficult for the SEC to identify and focus on the incidents that are actually significant and warrant SEC attention. As discussed below, the goals of the Proposed Rule could be better served by extending the proposed notification deadline by at least 24 hours and slightly changing the notification threshold.

Requiring notification within 48 hours will mean that Private Fund Advisers will be spending precious time in the first hours of an incident drafting a notification to the SEC (instead of dedicating resources to incident response); revising the disclosure as new information becomes available; and subsequently amending the original disclosure after submission when new facts emerge that render the original notification incomplete or misleading. Additionally, when a firm discloses to one regulator, it is customary that this regulator will ask about notification to other regulators. Firms typically make simultaneous disclosures to all of their regulators in order to avoid scrutiny by any one particular regulator for a delayed disclosure to that regulator. Because the SEC's 48-hour timeframe is materially shorter than the timeframe in which Private Fund Advisers generally provide notice of cyber incidents to state and federal regulators, the Proposed

[5] *Id.*

Rule will likely lead many Private Fund Advisers to draft similar notifications to other regulators in the same condensed timeframe, even if not required by those regulators, to avoid criticism for notifying some government agencies much earlier than others. Those other notifications will be similarly vague or inaccurate, and will need prompt updating or amending, further draining resources of the Private Fund Adviser or Covered Client that is responding to a data breach.

Providing at least an additional 24 hours to assess the incident will lead to more accurate and meaningful disclosures, and fewer placeholder disclosures to the SEC and other regulators for incidents that ultimately do not meet any notification threshold. Additional time also will provide Private Fund Advisers with the ability to respond to the incidents themselves and take appropriate steps in the best interests of protecting their clients, rather than spending their limited time and resources drafting and revising an SEC filing.

A 72-hour notification deadline is consistent with Part 500 of the New York Department of Financial Services cyber regulation (23 CRR-NY 500.17(a)), as well as the breach notifications to European regulators under Article 33 of the General Data Protection Regulation ("GDPR").

We also recommend that the SEC modify the definitions of "significant cybersecurity incident" and "substantial harm" to enumerate specific types of operational impacts that trigger the notification obligation, as well as to change the notification trigger from a "reasonable belief" that an incident has occurred to an actual "determination" that an incident has occurred. Without such clarifications, Private Fund Advisers are likely to both over-report and report vague information, which would not help the SEC in formulating an appropriate response. Further, additional time will provide Private Fund Advisers with the ability to respond appropriately and robustly to the incidents themselves and take appropriate steps in the best interests of their clients rather than spend limited time and resources compiling an SEC filing. Each of these proposed changes would improve the quality and accuracy of the notifications that the SEC will receive, reduce the number of meaningless or inaccurate placeholder notifications, and will strengthen the SEC's ability to evaluate and investigate cybersecurity incidents and any adverse impact on the marketplace.

III. Proposed Alternatives

Extended Timeline

As stated, the 48-hour reporting requirement does not serve the SEC's stated objectives. We believe that an extended reporting timeline to at least the 72 hours that is required for NYDFS Part 500 and GDPR notifications, would better serve the SEC's purpose to monitor cybersecurity risks at Private Fund Advisers. An additional 24 hours or more would provide Private Fund Advisers the time they will need to (1) determine whether a reportable incident has actually occurred, (2) develop relevant facts that are not likely to change in the near future, and therefore (3) draft a meaningful notification.

Clarifying the Notification Trigger

The SEC should also modify the definitions of a "significant cybersecurity incident" and "substantial harm" to enumerate specific types of operational impacts that will trigger the

notification obligation. For example, the new 36-hour breach notification rule for financial institutions (12 CFR 225 (Federal Reserve System); 12 CFR 53 (Department of the Treasury); 12 CFR 304 (FDIC)) has an "operational impact" trigger that is limited to, among other things, incidents that affect "a material portion of [a covered entity's] customer base." The current draft of the Proposed Rule, by contrast, suggests that substantial harm to even one client or investor in a private fund (such as significant monetary loss or the theft of personally identifiable or proprietary information) would be a sufficient trigger for notification to the SEC.[6] It is therefore unclear whether any non-trivial financial loss to an investor, even if subsequently reimbursed by a Private Fund Adviser or Covered Client, would be sufficient to trigger the notification obligation.

The SEC should also change the notification trigger from a "reasonable belief" that an incident has occurred to a "determination" that an incident has occurred, to avoid confusion over what would constitute a "reasonable belief," which is likely to lead to the flood of placeholder notifications discussed above. It is likely for this reason that the Department of Treasury, Federal Reserve, and FDIC made a similar change to their draft notification rule, which initially had a "good faith belief" trigger (86 FR 2299 at 2300), and ended up with a "determination" trigger in the final regulation. 12 CFR 225.302 (Federal Reserve System); 12 CFR 53.3 (Department of the Treasury); 12 CFR 304.23 (FDIC); 86 FR 66424 at 66430 ("After considering the comments carefully, the agencies are replacing the 'good faith belief' standard with a banking organization's determination. The agencies agree with commenters who criticized the proposed 'believes in good faith' standard as too subjective and imprecise").

*****

The AIC appreciates the opportunity to comment on the Proposed Rule and would be pleased to answer any questions that you might have concerning our comments.

Respectfully submitted,

Jason Mulvihill
Chief Operating Officer and General Counsel
American Investment Council

[6] Proposing Release at 13537.