CAMBRIDGE

VIA ELECTRONIC MAIL: rule-comments@sec.gov

April 08, 2022

Vanessa A. Countryman, Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-0609

Re: **File No. S7-04-22**

Dear Ms. Countryman:

Cambridge Investment Research Advisors, Inc. ("CIRA"), a Securities and Exchange Commission ("SEC" or the "Commission") registered investment adviser ("RIA"), appreciates the opportunity to comment on the proposed rules regarding Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (the "Release"). Technology plays an increasingly important and pervasive role in the financial services industry, and in the relationships among regulators, firms and the investing public. Against that backdrop, it is important that the SEC and firms like CIRA coordinate the industry's approach to cybersecurity risk identification, management, and response. A unified, collaborative approach serves the Commission and the firms' interests in, as well as commitment to, protecting investors through reasonable, appropriate, and clearly defined policies and procedures to address cybersecurity matters.

Investors are best served when the Commission and RIAs collaborate and the frequency of cyber-attacks, and the diversity of bad actors, compels an urgency in reaching a collaborative industry approach. To that end, CIRA supports the goals of the Commission but requests the Commission consider the following recommendations and concerns related to the proposed Release.

I. Placement of the Proposed Cybersecurity Rules Under the Anti-Fraud Provisions

The Commission and all industry participants, including the public, would be best served if the Commission incentivized RIAs to report material cyber events, rather than enforcing new standards through the anti-fraud provisions of the SEC rules. As such, the requirement to develop policies and procedures designed to address cybersecurity incidents should not be tied to the anti-fraud provisions created under 15 U.S.C. §80b-6(4). The anti-fraud provisions are designed to prevent fraudulent acts. In situations where a material breach of a technology system has occurred,

the hacker commits the fraudulent act. The hacked individual or entity is the victim of the fraudulent act. No individual or entity seeks to be hacked.

Consistent with CIRA's view, in her Statement on Cybersecurity Risk Management for Investment Advisers, Commissioner Peirce opines that an adviser's system that has been successfully breached should not lead us to the conclusion that the adviser was lax in its efforts to protect investors' data. Moreover, as the Commission correctly notes, even adequately prepared RIAs are not immune from attack, as "even the best preparation may not be effective against such exploits."

Where an RIA employs reasonable measures to prevent or prevail against known risks but falls short as a result of an unknown vulnerability, such failure is not the result of "any act, practice, or course of business which is fraudulent, deceptive, or manipulative" under Section 206(4). Therefore, CIRA advocates for the use of the Commission's general rulemaking to motivate RIAs to comply with the reporting requirements rather than to punish RIAs for complying with the reporting requirements under the anti-fraud provisions.

Additionally, the framework created by the language of proposed rule 206(4)-9(a), which states that "it is unlawful for any RIA … to provide investment advice to clients unless the adviser adopts and implements written policies and procedures that are reasonably designed to address the adviser's cybersecurity risks" is unreasonable and disconnected from the statutory requirements of investment advice. That an RIA would be engaging in "fraudulent, deceptive, or manipulative acts, practices, or courses of business" because the Commission determines that RIA's cybersecurity policies and procedures are insufficient, resulting in a material breach, is distinct from providing investment advice. The purpose of the proposed mechanism and the Commission's efforts related to the reporting of material breaches is better served without tying effective cybersecurity policies and procedures to investment advice.

While practices employed by some RIAs may not sufficiently address the Commission's investor protection concerns, it is the exceptional case where that failure is intentional or reckless. Consequently, CIRA encourages the Commission to reconsider its position and address cybersecurity policies and procedures under Section 204 as opposed to Section 206.

II. CYBERSECURITY PRACTICES AND STANDARDS

Implementation of effective, robust cybersecurity standards, measures, and practices is an appropriate and laudable industry goal. The Commission has recognized differences among firms' businesses by contemplating latitude in the construction and implementation of tailored policies and procedures. Nevertheless, while the language of proposed rule 206(4)-9(a) is broad, it is highly prescriptive. Here, an RIA is not given the flexibility to actually tailor rules to its business but rather faces some exacting thresholds and standards.

While the Commission acknowledges that a "one-size-fits-all" approach may not work, the proposed framework imposes precisely such an approach. Instead, the Commission should develop materials to support the creation of policy and procedure "best practices," as well as provide guidance regarding how to implement those best practices within the limitations of each firm's unique business structures.

CIRA asks the Commission to re-evaluate the approach espoused in the proposed rule regarding adequate policies and procedures. The Commission should consider creating materials to guide firms' efforts to implement structures that will allow them to withstand cyberattacks and address cyber incidents, rather than compel firms to implement policy and procedure steps that may not actually address their vulnerabilities and cybersecurity concerns.

III. CYBERSECURITY INCIDENT REPORTING

The Commission proposes that RIAs report certain cyber events on Form ADV-C within 48 hours after having a reasonable basis to conclude that a significant adviser cybersecurity incident occurred or is occurring. The proposed rule defines a significant adviser cybersecurity incident as a cybersecurity incident, or a group of related incidents, that significantly disrupts or degrades the adviser's ability to maintain critical operations (including but not limited to investment, trading, reporting, and risk management of the adviser), 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, or (2) substantial harm to a client whose information was accessed.

While CIRA agrees with the SEC on the importance of client disclosures related to cybersecurity breaches, the 48-hour timeframe is unreasonable, as the application of this reporting standard is too near in time to a possible cybersecurity incident. The requirement to simply report something within a 48-hour timeframe does not contemplate the impacts of other potential legal requirements (such as restrictions that may be imposed by law enforcement or other agencies, both at the state and federal levels) or the likelihood that an RIA may not have a sufficient understanding of the nature and scope of the incident to even know that they need to report it.

The proposed rule creates a conflict between the appearance of the RIAs adequacy of cybersecurity measures and the Commission's desire to track the occurrence of cyber incidents. This conflict is reflected in the fact that the proposed rule would require RIAs to report each cybersecurity incident when the incident results in a significant disruption or degradation of the adviser's ability to maintain critical operations. This standard raises the question, to what degree is a disruption or degradation of a system "significant"? The example provided in the Release describes an incident where an entire email system fails, presumably during market hours, as the result of a malware attack. It is unclear from the proposed language whether an email failure will always result in "the disruption or degradation of the RIA's ability to maintain operations," or whether such an event precludes the RIA from maintaining its critical operations during or after an event. An RIA may timely employ remedial measures sufficient to avoid a "critical operations" impact. If the incident lasted a total of ten minutes only, the Commission seems to imply that the incident may not need to be reported. However, the strict language of the proposed rule, requiring that any significant disruption of the adviser's ability to keep its email functionality online, regardless of the amount of time, would require the RIA to report the incident. In instances like this, some RIAs may view it to be in their best interest to refrain from reporting the event in order to be viewed by the SEC and the investing public as an RIA whose cybersecurity measures are effective. However, knowledge of the incident just described might be useful for the Commission in order to understand the nature and frequency of these types of events.

Rather than creating a framework where RIAs would either fear underreporting (and thus report every incident regardless of significance) or fear reporting an incident because of the negative implications of a reported incident (and thus not report the incident at all), the Commission should provide greater guidance and examples regarding the meaning of the term "significant" under the proposed rule so that RIAs would know when there would be no obligation to report minor or insignificant incidents, and when to report those the Commission is actually concerned about.

The proposed rule also requires an RIA to report an unauthorized access or use of the RIA's information that results in substantial harm to the RIA or its clients. Here, the SEC includes the loss of a client's personally identifiable information. This reporting requirement raises the question of degree – what is "substantial"? A definition of "substantial" would provide greater reporting clarity. Moreover, while informative, the reference to Regulation S-P does not clarify this ambiguity. For example, if an RIA associated representative experienced an email compromise where five client email addresses were accessed by unauthorized means, would that be enough to warrant filing a notice?

While the two-pronged approach illustrated in the proposed rule language captures incidents and informs industry participants, the lack of specificity in the proposed language may prove misleading. Further, ambiguity in the terms and requirements of the proposed rule fosters misapplication. For this reason, CIRA requests the SEC review these terms, considering the points above, and consider amending the proposed rule language for greater clarity or provide interpretive guidance giving greater explanation regarding how and to what degree the rule will be applied.

CIRA also challenges the suggestion that an RIA is a "bad actor" if it is the victim of numerous cybersecurity attacks. The Commission notes in the Release that investors will be able to make more informed decisions about those RIAs with whom they may do business by the number and description of cybersecurity incidents reported. Under the presently proposed language, a likely outcome will be certain RIAs underreport or decline to report incidents entirely, while others RIAs seeking diligent compliance with the proposed rule will report most, any and every appearance of a cyber incident. The potential impact of this may be the underreporting and, arguably, non-compliant RIAs would be rewarded by clients' and prospective clients' inaccurate perception of underreporting firm's cybersecurity while RIAs seeking to comply with the proposed rule would be punished with an inaccurate reputation as lacking in sufficient cybersecurity protocols.

The length and breadth of potential cyberattacks covers multiple scenarios with complexities beyond the currently proposed standard. The absence of clear standards for what should be reported creates confusion and thus inadvertently may result in non-compliance. The resulting "enforcement as guideline" type regulatory environment would not be an effective approach to address cybersecurity vulnerabilities and issues as it would not serve the needs of investors and RIAs or fulfill the Commission's purpose for the reporting mechanism.

While CIRA appreciates the complexities of identifying the types of cybersecurity events that warrant reporting, greater clarity in the proposed rule enhances the likelihood of achieving a reporting system that meets the needs of investors, the industry and the Commission. In this regard, the Commission should articulate characteristics of those events that should be reported and afford

a degree of latitude with respect to the time frame within which to report such events. This proposed enhancement to the rule furthers a collaborative approach to this important issue.

IV. THIRD-PARTY CONTRACTUAL RELATIONSHIPS

The Commission notes that the requirements of the proposed rule may impact existing contracts for information technology services. CIRA asks the Commission to further consider its position relating to contracts with third-party vendors. Many RIAs contract with third-parties for services like those described in the Release. Those agreements may not be terminable at the will of the RIA. This would place these RIAs in an untenable situation: having to choose between possibly taking a financial loss for early termination of a legally binding agreement, and risking a regulatory violation for failure to fully comply with the proposed rule. Given this, CIRA requests the Commission consider adding language to allow those RIAs time to implement reasonable solutions and bridge the gaps with these service providers or, at a minimum, allow RIAs the opportunity to enact lesser mitigation measures in order to bridge the gap. The possibility that an RIA would be obligated by the Commission to suffer a financial loss related to terminating a vendor contract seems counterintuitive and likely not the intended result of the Commission's proposed rulemaking.

V. UNIFORMITY WITH OTHER LAWS

Many firms like CIRA have affiliated or dually registered broker-dealers, that are subject to FINRA-specific cybersecurity requirements. Additionally, RIAs are also subject to many state specific privacy and cybersecurity laws. Lastly, President Joe Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") on March 15th of 2022. As a result of these various obligations, CIRA suggests the Commission consider uniformity as much as possible while incorporating input through this comment process. Specifically, with respect to CIRCIA, considering the inclusion of financial service companies, including broker-dealers and possibly investment advisers, within the scope of this new law, CIRA requests the Commission contemplate the exclusion of registered investment advisers from the proposed cybersecurity reporting rule and amend the language to apply to the Investment Company Act of 1940, as applicable. If a general exclusion is not granted, then CIRA requests the SEC include a provision excluding those RIAs that are affiliated with broker-dealers subject to the CIRCIA.

CIRA appreciates the opportunity to offer comments regarding the Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies Release.

Sincerely,

/s/ *Seth Miller*

Seth Miller
General Counsel
Chief Risk Officer