Cambridge Investment Research, Inc.
Cambridge Investment Research Advisors, Inc.
1776 Pleasant Plain Road
Fairfield, IA 52556
Phone: 641-472-5100
Facsimile: 641-469-1687
Member FINRA/SIPC

June 5, 2023

Via Electronic Mail (**rule-comments@sec.gov**)

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

Re: Release Nos. 33-11028; 34-941917; IA5956; IC-34497; File No. S7-04-22 Release Nos. 33-11167; 34-97144; IA-6263; IC-34855; File No. S7-04-22 Cybersecurity Risk Management Rules for Investment Advisers, Registered Investment Companies, and Business Development Companies ("IA Proposal") Release Nos. 34-97141; IA-6262; IC-34845; File No. S7-05-23 Regulation S-P: Privacy of Consumer Financial Information and Safeguard Customer Information ("Reg S-P Proposal") Release No. 34-97142; File No. S7-06-23 Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents ("BD Proposal")

Dear Ms. Countryman:

Cambridge Investment Research Advisors, Inc. ("CIRA"), a Securities and Exchange Commission ("SEC" or the "Commission") registered investment adviser ("RIA"), and its affiliated broker-dealer, Cambridge Investment Research, Inc. ("CIR") (collectively "Cambridge"), appreciate the opportunity to comment on the proposals referenced above (collectively the "Proposals").

On March 15, 2023, the Securities and Exchange Commission ("SEC") published the Proposals. Cambridge understands and concurs, conceptually, with the SEC's goal to reinforce protections afforded investors, market participants, and the financial services industry with respect to a rapidly increasing number of attempted cyber intrusions and attacks, as well as to

address the more general risk of unauthorized access to customer information. These considerations clearly play an increasingly important and pervasive role of technology in the financial services industry.

Against that backdrop, it is critical that regulators, firms, and the investing public mount and coordinate the 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 served best when the Commission and RIAs collaborate. Moreover, the frequency of cyber-attacks and the diversity of bad actors compel an urgency in reaching a collaborative industry approach to matters of this type. To that end, Cambridge supports the goals of the Commission but requests that the Commission consider the recommendations and concerns outlined below and related to the Proposals. These concerns are supplemental to Cambridge's comment letter of April 8, 2023.

I. SUMMARY OF PENDING RELEASES

The requirements reflected in the Proposals, as embodied within several Releases, generally fall into four categories: (1) cybersecurity policies and procedures, (2) reporting and notification obligations, (3) disclosure requirements, and (4) books and records requirements.

Cambridge's comments regarding these four matters can be summarized as follows:

- Adoption of any Proposal should be accompanied by an extended and individualized implementation period;
- The Proposals should be aligned with existing incident reporting and data privacy regimes as well as aligning the Proposals to each other where appropriate;
- The Reg S-P notification requirement period should be expanded from "not later than 30-days" to "not later than 60-days" and triggered when a firm becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to occur.
- The immediate reporting requirement contained in the BD Proposal is not practical and should be extended;
- The 48-hour reporting requirement contained in the IA Proposal is not practical and should be extended;
- The various SEC-compelled disclosure forms (SCIR-I and II, ADV-C and ADV

Part 2A) should be consolidated into a single form.

- Finally, in light of the complex, inter-related nature of the Proposals, they should not be adopted without an additional and more focused comment period.

I. THE PROPOSALS' INTERRELATED COMPLEXITIES COMPEL AN EXTENDED IMPLEMENTATION PERIOD.

Regulation S-P ("Reg S-P") imposes certain reporting requirements with respect to impacted clients, which differ from the reporting requirements contemplated by the Proposals.

A. MINIMUM NOTIFICATION OBLIGATIONS ARE APPROPRIATE

As Cambridge interprets the Proposals, they encompass both notification obligations and definitions applicable to those obligations. These obligations and definitions need to work in conjunction with existing requirements and to permit firms to leverage their existing Reg S-P compliance framework.

It is appropriate that the notification requirement under the Reg S-P Proposal applies if a firm determines that the client information at issue was neither actually nor reasonably likely to be used. However, "use" of the information could benefit from additional specificity. Specifically, the addition of the "inconvenience" element is not necessary, as use of the phrase "more than trivial" suffices to evidence the "substantial harm" referenced in the Proposal.

In addition, the 30-day notification period is too short. Once a firm becomes aware of unauthorized access to or use of customer information, the firm needs sufficient time to review and evaluate the underlying facts. A period of, for example, 60 days would be more realistic, while achieving the Proposals' same goals.

In assessing firms' responsibilities, the SEC should not lose sight of the impact of the overlay of various state requirements with which firms will still need to comply. This additional burden should bear on the SEC's determination of appropriate implementation periods, as it will require reconciliation of data privacy and incident notification programs for federal and state purposes.

B. THE INTERRELATED NATURE OF THE PROPOSALS COMPEL AN EXTENDED COMMENT PERIOD

The SEC extended the Comment Period for the IA Proposal. A similar extension is appropriate with respect to the other components of the Proposals given the interrelated nature of the components of the Proposals.

Moreover, for firms such as Cambridge, which operates both a BD and an RIA, the significant burden to bring both entities into compliance necessitates that the implementation period for the Proposals be extended. This will afford dual registrants and those firms operating dual business models an opportunity to modify both entities' compliance frameworks and to identify some synergies that might make compliance more effective and economical.

II. INCIDENT REPORTING SHOULD BE STANDARDIZED AND STREAMLINED

The Reg S-P Proposal applies to both broker-dealers and advisory firms. Consequently, as currently drafted, the Proposals render reporting by a broker-dealer potentially duplicative of the advisory firm's reporting. Modification of the Proposals to streamline reporting obligations for dual-registrants and those firms operating both a BD and an RIA is appropriate.

Additionally, while prompt reporting of a cybersecurity incident is important for the protection of all industry participants, the need for prompt reporting must be balanced against practical consideration.

C. NEITHER IMMEDIATE REPORTING FOR BROKER-DEALERS NOR THE 48 HOUR REQUIREMENT APPLICABLE TO THE ADV-C ARE PRACTICAL

To mandate immediate incident reporting, or even to compel reporting within 48 hours, denies firms a meaningful opportunity to determine, much less assess, the facts of a particular situation. This rushed reporting requirement is inconsistent with the need for accurate and specific discovery of the *facts*, and thus does not further the underlying goal of providing industry participants with the information necessary to respond meaningfully to a particular cyber incident.

Cambridge agrees with the Commission on the importance of client disclosures related to cybersecurity breaches. However, a 48-hour reporting timeframe is unreasonable, as it requires reporting too near in time to a possible cybersecurity incident. The requirement to simply report something within a 48-hour timeframe ignores 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 the firm may lack a sufficient understanding of the nature and scope of the incident to even know that it needs to be reported.

Moreover, the Proposals could require firms to report a cybersecurity incident without sufficient information to assess the scope or degree (i.e., "significance") of any disruption or degradation of a firm system. Furthermore, there could be instances where it is in the best interests of all concerned to refrain from public reporting of any event where it could afford the wrongdoer information necessary to further their scheme.

Rather than compelling unnecessarily rushed, bifurcated, and potentially incomplete reporting, Cambridge supports the use of a single, two-part form for the reporting of cyber incidents. The form contemplated herein would encompass aspects of the current SCIR-I and Form ADV-C. It should be submitted through the CRD/IARD system.

The proposed two-part form allows for the submission of confidential information necessary to permit the appropriate industry regulators to perform their function. Additionally, a single form would allow firms to submit information just once, as opposed to submitting separately for the affiliated broker-dealer and advisory firm.

Moreover, the event disclosure should afford the reporting firm appropriate protections that reflect the evolutionary nature of the investigation process. It takes time following discovery of a cyber event to determine the facts, assess the scope of any intrusion, and outline a course of action. A safe harbor to allow for continued discovery and reporting is necessary to incent meaningful efforts to continue to gather and evaluate evolving facts relevant to an incident.

III. DISCLOSURES AND THE RISK ASSESSMENT PROCESS SHOULD BE STREAMLINED

The second part of the consolidated Form SCIR contemplated above would be the public-facing disclosure. This would encompass the Form SCIR-II and ADV-2A incident related disclosures.

Similar to Section II above, this portion of the consolidated form allows for streamlined reporting for dual registrants and firms operating two independent models of known facts necessary to put industry participants on notice of an incident, as well as to afford those participants with the information necessary to permit them to meaningfully protect their interests.

Affiliated entities could use a single form to allow more timely, consistent reporting of an event. The rationale underlying the proposed use of a single form has parallels to the adoption of a single Form CRS.

IV. THIRD-PARTY SERVICE PROVIDERS

The Commission's Proposals contemplate the use of third-party service providers, so long as they are "appropriately overseen." The use of such providers is common and usually arises from a written contract. Those agreements may not be terminable at the firm's will. This would place the firm 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, Cambridge requests that the Commission consider adding language to allow firms time to implement reasonable solutions and bridge the gaps with

these service providers or, at a minimum, allow firms the opportunity to enact lesser mitigation measures to bridge the gap. The possibility that the Commission would obligate a firm 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

Firms such as Cambridge are also subject to RIA-specific and FINRA (or BD)-specific cybersecurity requirements, in addition to all firms being 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 15, 2022. As a result of these various obligations, Cambridge suggests that the Commission consider uniformity as much as possible while incorporating input through this comment process. Specifically, with respect to CIRCIA, the Commission should consider the inclusion of financial service companies, including broker-dealers and possibly investment advisers, within the scope of this new law, while making accommodations for firms operating both a BD and an RIA.

VI. CONCLUSION

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

Sincerely,

/s/ *Seth A. Miller*

Seth A. Miller
President Advocacy & Administration
General Counsel

1776 Pleasant Plain Road | Fairfield, Iowa 52556 | Phone: 800-777-6080 | Fax: 641-469-1691
Email: cambridge@cir2.com | Website: cir2.com