April 26, 2023

Via Electronic Submission

Ms. Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC
20549-1090

Re: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period (SEC Rel. Release Nos. 33-11167; 34-97144; IA-6263; IC-34855; File No. S7-04-22)

Dear Ms. Countryman,

I submit these comments on the Commission's proposal (the "Proposal") that would require registered investment advisers, registered investment companies, and business development companies (collectively, the "Registrant(s)"), subject to the reporting requirements under the Securities Exchange Act of 1934, to adopt and implement polices "reasonably designed to address cybersecurity risks."[1] As a first-year law student who is interested in the investment management industry and who is concerned about the heightened risk of cybercrime, I am broadly in favor of the Proposal. I believe that it represents a conscious decision by the Commission to tackle an ongoing problem confronting the entire digital world, and I believe the Commission has appropriately identified an area ripe for appropriate rulemaking. However, I have two topics that I believe that the Commission should confront and consider more fully before implementing the proposed rules, and I would like to add my full support for another

[1] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 13524, 13524 (Mar. 9, 2022) available at: https://www.federalregister.gov/documents/2022/03/09/2022-03145/cybersecurity-risk-management-for-investment-advisers-registered-investment-companies-and-business (**Proposal**).

aspect of the Proposal, with one specific area where I would respectfully request additional clarification.

INTRODUCTION

The Commission issued a Notice of Proposed Rulemaking asked for public comment on March 9, 2022, titled: "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies." The Proposal was then reopened for comment on March 23, 2023, in a notice titled: "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period." The Proposal seeks to tackle an important issue that plagues not only the investment management industry, but the entire economy: the risk of devastating cyberattacks.

A cyberattack has the power to impact not just a Registrant's bottom line, but it also has the potential to put at risk and decimate the savings of individuals who rely on Registrants to manage and grow their money.[2] Furthermore, cyberattacks can be particularly devastating for smaller firms and can be so severe that they may go out of business as a result.[3] Additionally, our world has changed drastically in the wake of the COVID-19 pandemic, and we have seen a marked shift to firms allowing more remote work – in effect, permitting employees more flexibility (for better or for worse) in their cybersecurity protections.[4] In wading into these waters, the

---

[2] 2022 Investment Company Factbook, INVESTMENT COMPANY INSTITUTE (2022), available at: https://www.icifactbook.org/pdf/2022_factbook.pdf (finding that households make up the largest group of investors in mutual funds managed by registered investment companies and that these firms managed "23 percent of household financial assets at year-end 2021").

[3] Alex Halperin, *Worried About a Cyberattack? What It Could Cost Your Small Business*, BND (Feb. 21, 2023) https://www.businessnewsdaily.com/8475-cost-of-cyberattack.html (finding that in 2019 43% of data breaches affected small businesses who may be unable to shoulder the costs of remediation).

[4] Mark Nevins, *New Dangers of Working From Home: Cybersecurity Risks*, FORBES (May 19, 2021, 9:18 PM), https://www.forbes.com/sites/hillennevins/2021/05/19/new-dangers-of-working-from-home-cybersecurity-risks/?sh=96f532422fb1 (finding that remote work poses unique cybersecurity risks to companies – focusing

Commission has signaled its commitment to tackling an important issue that has ripple effects throughout our entire economy.

I strongly support the Proposal, but I would urge the Commission to conduct additional consideration on two important topics, and I would like to underline my support and wish for added clarity on one further topic:

1. **The Commission should consider tailoring the proposed requirements to the size of the Registrant in question to avoid unduly burdening smaller firms.**

2. **The Commission should amend its plan to require that Registrants publicly disclose certain details regarding significant cybersecurity incidents.**

3. **The Commission should require that a Registrant's board of directors approve and review annually its cybersecurity policies, and the Commission should provide additional clarification on the board's role in oversight.**

BACKGROUND

Cybercrime has increasingly become a large threat to the investment management industry, and cybersecurity is among one of the most critical issues for U.S.-based investors – with data suggesting that incidents can severely impact a firm's stock price and an investor's returns.[5] The "average cost to an organization for a single cyber incident now exceeds $1 million[;]" furthermore, following a public cyberattack, customers are increasingly apt to lose faith in the affected organization and are 33% more likely to "[discontinue] their relationship with the organization."[6] While the industry generally lacks the same "public-facing infrastructure" as

primarily on risks posed by third-party productivity digital applications that have the "bare minimum of security settings").

[5] See 2019 Responsible Investing Survey Key Findings, RBC GLOB. ASSET MGMT (2019), available at: https://global.rbcgam.com/sitefiles/live/documents/pdf/rbc-gam-responsible-investing-survey-key-findings2019.pdf; see also Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, & Rene M. Stulz, *Risk management, firm reputation, and the impact of successful cyberattacks on target firms*, 139 J. OF FIN. ECON. 747, 749 (2021).

[6] Mutual Fund Directors Forum – Cybersecurity and the evolving threat landscape, DELOITTE DEVELOPMENT LLC (2022), available at: https://www2.deloitte.com/us/en/pages/advisory/articles/asset-management-firms-facing-higher-cybersecurity-risk.html; see also Miloslava Plachkinova and Chris Maurer, *Teaching Case: Security Breach at Target*, 29 JOURNAL OF INFORMATION SYSTEMS EDUCATION 11, 14 (2018) (finding that after Target was victim of

other areas of the economy (*e.g.*, online shopping platforms), which has made it historically isolated from threats, as cybercriminals continue to develop new techniques and other sectors beef up their defenses in light of recent, highly-public attacks, the investment management industry may become a more appealing target.[7]

Registrants are tempting targets for cybercriminals as many possess "highly valuable intellectual property" in the form of proprietary investment strategies, and they are the guardians of immense amounts of capital.[8] For example, as of 2021, the investment adviser industry had $128.4 trillion in assets and provided services to 64.7 million clients.[9] Furthermore, Registrants often rely on third-party service providers to act as "custodians, distributors, administrators, transfer agents[,]" etc., and these third-parties are likely to have access to data critical to both investors and Registrants themselves.[10] Data suggest that 63% of cybersecurity breaches are linked to a third-party service provider – further underlining the need for the Commission to examine and impose new regulation on this issue.[11]

While cyberthreats remain potent risks to firms, I believe it is most important to highlight that the investment management industry holds a unique position in our economy: that as the guardians and protectors of many individuals' savings, retirement accounts, and personal financial information. For example, as of 2022, 52.3% of households in the United States owned mutual funds, a product commonly offered by Registrants, and 2/3 of those owners were individuals

---

a massive cyberattack in Q4 of 2013 the company experienced a massive loss of customer confidence and a 34.3% decrease in net revenue from 2012 to 2013).

[7] Closing the gap – Cyber Security and the asset management sector, KPMG LLP (2018), available at: https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2018/01/closing-the-gap-cyber-security-asset-management.pdf.

[8] Id.

[9] Snapshot 2022, INVESTMENT ADVISER ASSOCIATION (2021), available at: https://investmentadviser.org/wp-content/uploads/2022/06/Snapshot2022.pdf.

[10] Cybersecurity and the evolving threat landscape, Deloitte; see also The Cost of Third-Party Cybersecurity Risk Management, PONEMON INSTITUTE LLC (Mar. 2019), available at https://info.cybergrx.com/ponemon-report.

[11] The Cost of Third-Party Cybersecurity Risk Management, PONEMON INSTITUTE LLC.

households making less than $150,000 a year – making the industry the custodians of a "key component of the household balance sheet for millions of Americans" – not just those from the upper echelons of the socio-economic ladder.[12] These mutual funds then make up the primary securities held by retirement investment accounts – further underlining the immense importance of implementing regulations to protect this capital from cybercrime.[13]

The Commission's Director of the Division of Investment Management, in a recent address to industry leaders, has further highlighted the need to confront issues surrounding cybersecurity.[14] Director Birdthistle noted that while technological advancements have brought "many positive improvements" to the industry, they also present new challenges and risks that Registrants, and the Commission, must confront head on to combat the "technology-related perils of our time."[15] The Director's candor in acknowledging the potent threat posed by cybercrime further underlines the necessity for these proposed regulations to be put in place.

Because of the Registrants' incredibly important status within our economy and the rapidly increasing threat posed by cybercrime, the Commission should work to implement rules, in line with its *stated mission*, that seek to "protect investors" and to ensure that the "[facilitation] of capital formation" is accomplished in a manner that both considers and adapts to our increasingly digitally connected world.[16]

---

[12] Mutual Funds Are Key to Building Wealth for Majority of US Households, INVESTMENT COMPANY INSTITUTE (Oct. 31, 2022), https://www.ici.org/news-release/22-news-ownership.
[13] See id.
[14] William Birdthistle, *Remarks at the ICI Investment Management Conference*, U.S. SECURITIES AND EXCHANGE COMMISSION (March 20, 2023), https://www.sec.gov/news/speech/birdthistle-remarks-ici-investment-management-conference-032023.
[15] Id.
[16] *What We Do*, U.S. SECURITIES AND EXCHANGE COMMISSION (April 6, 2023), https://www.sec.gov/about/what-we-do.

PROPOSED COMMENTS

1 The Commission should consider tailoring the proposed requirements to the size of the Registrant in question to avoid unduly burdening smaller firms.

The investment management industry is varied and dynamic and firms range in size from small family-run offices to massive multinational corporations. In 2021, approximately 90% of the 14,806 SEC-registered investment companies were classified as "small businesses employing fewer than 50 people."[17] These firms represent a large swath of the industry that may not have massive compliance, risk management, and cybersecurity teams on their payrolls. While close to 2/3 of all assets managed by Registrants are managed by the 210 largest firms, it is imperative that the Commission not lose sight of these smaller firms who continue to provide essential financial services to communities and businesses across the nation.[18]

The Proposal notes that it would require all Registrants to implement cybersecurity policies that would, among other things, require that there be "written contracts" between a Registrant and a third-party service provider reflecting the latter's cybersecurity programs.[19] While this would undoubtedly provide an additional layer of protection to ensure that firms are implementing strategies that take into account the risks of sharing data with third-parties, I do not believe the Proposal appropriately considers the burden these requirements may place on smaller advisers. While larger Registrants may have the bargaining power to effectively force a service provider to include details of their cybersecurity programs in the written contract between the two parties, smaller Registrants may lack leverage in ensuring the inclusion of such a requirement and may be forced to agree to contracts simply to remain in business. Many smaller Registrants lack agency in the negotiation process and are often forced to simply agree to the

[17] Snapshot 2022, INVESTMENT ADVISER ASSOCIATION.
[18] Id.
[19] **Proposal** at 13550.

contract offered or risk losing an essential service needed for their longevity (*e.g.*, fund distribution services).

While I generally support increased oversight of these third-party providers, I am concerned that the Commission may be unrealistic in its proposed regulations. The Commission does optimistically note that the "costs associated with negotiating such contractual provisions may also be partly borne by service providers[;]" however, they then note that these costs could also be shouldered by "clients and investors".[20] This apparent comfort with immediately passing on increased costs to clients and investors seems an odd position for the Commission to take. While it may be easier for larger Registrants to bear these costs, smaller firms may have no choice but to drastically increase service fees and other prices – potentially losing business in the process. The Commission should instead focus its energy on ensuring that other entities under its jurisdiction (*e.g.*, broker dealers, bank custodians, transfer agents – all quintessential third-party service providers) are held to increased cybersecurity requirements as well.

2 The Commission should amend its plan to require that Registrants publicly disclose certain details regarding significant cybersecurity incidents.

The Proposal admirably attempts to address the fact that many material cybersecurity incidents are underreported, as firms are loath to be in the negative national spotlight and, as previously mentioned, do not want to lose investor's confidence. Requiring reporting would mandate compliance and ensure better awareness of cyberthreats. However, I do not believe that the proposed reporting mechanism is the most effective or the most secure method for the Commission to implement.

The Proposal would require Registrants to file a new Form ADV-C detailing "cybersecurity incidents" within 48 hours of a "significant" breach and would require the form to be amended

[20] **Proposal** at 13551.

when "information reported previously becomes materially inaccurate or if new material information is discovered."[21] I am concerned that the proposed form may be giving cybercriminals a free notice letting them know of the extent of their success. The Form ADV-C would require Registrants not only to inform that an incident had occurred, but it would also require them to report the "nature and scope of the significant cybersecurity incident" and whether the incident was "covered under a cybersecurity insurance policy."[22] If reported truthfully, the "nature and scope" question on the form would provide cybercriminals with an in-depth analysis of their penetration into a firm's digital resources – essentially creating a map of their triumph. While I believe that the Commission must require that investors be made promptly aware of cyberattacks, I am hesitant to mandate that such in-depth reporting be made public on the Commission's EDGAR portal.

Furthermore, such a stringent reporting timeframe might again have an undue effect on smaller Registrants. While attacks on smaller firms can be devastating, they are unlikely to have the same market-wide effect as an attack on a much larger Registrant, thus, they should be held to a slightly different standard than their larger, more liquid peers. The Commission could consider amending its required reporting timeframe for firms with only a certain amount of assets under management. For example, changing the 48-hour reporting window to 72 hours could allow a smaller firm's cybersecurity team to tackle the issue more effectively, and the Commission should not sacrifice quantity of reports for quality.

In sum, I do believe that the Commission should mandate that Registrants report incidents, both to the government and to the public, to better understand cybercrimes and to inform investors of risks to their finances. However, I would contend that they should be required to

[21] **Proposal** at 13554.
[22] Id. at 13595.

publicly note *only* whether an incident has occurred, whether any essential data has been compromised, and whether they have been successful in remediating the attack. Registrants should then be required to *privately and securely* disclose much more information to the Commission so that the agency can learn about the crimes and work the Registrant to better develop appropriate measures to prevent future incidents.

3 The Commission should require that a Registrant's board of directors approve and review annually its cybersecurity policies, and the Commission should provide additional clarification on the board's role in oversight.

The Commission acknowledges that cybersecurity is a top priority for boards of directors and, while "directors are not responsible for specifically designing or overseeing a cybersecurity program[,]" the board "must remain vigilant and ask key questions" to stay in line with the risk oversight that is statutorily required of fiduciaries.[23] The proposed rule 38a-2 would require a Registrant's board of directors to "initially approve...[any] cybersecurity policies and procedures" proposed by management and would ensure that any material changes to the plans and any cybersecurity incidents are "reviewed annually."[24]

Mandating that these procedures be put in place would ensure that directors "familiarize" themselves with the specific policies and procedures, and it would ensure that directors are engaged in discussions surrounding cybersecurity – making them more wary and better prepared to adapt if/when a cybersecurity incident occurs.[25] Furthermore, in a world where cyberattacks are happening with more frequency, the Commission's proposals ensure that boards adhere to their state-mandated responsibilities of both a "duty of care" and a "duty of loyalty" to the

[23] Mutual Fund Directors Forum – Cybersecurity and the evolving threat landscape, DELOITTE DEVELOPMENT LLC.
[24] **Proposal** at 13534.
[25] Id.

Registrant they serve.[26] By requiring these specific board-related proposals, the Commission is effectively ensuring that Registrants' boards confront these issues head on so that they can prove that they have backed up their decisions with sufficient information if confronted with the threat of litigation.

I would also ask that the Commission further clarify its language requiring that "[b]oard oversight not be a passive activity" – as this appears to wade into decision-making waters more appropriate for a Registrant's management and not a Registrant's board.[27] The Commission should clarify its language to confirm that boards remain focused on oversight and fostering insightful discussion – not on making management decisions.

CONCLUSION

The Proposal is an important step in confronting the terrifyingly potent issues posed by cyber-crimes. The proposed regulations work to ensure that investors are better informed of risks, and it confronts an area where "no Commission rules" currently exist.[28] By further considering the effects on smaller Registrants and slightly amending the materials that should be included on the Form ADV-C disclosure, the Commission can work to ensure that firms and the wider public are better informed and, overall, better protected. Additionally, by requiring that boards of directors confront cybersecurity issues head-on, the Commission has effectively demanded that these discussions take place at the highest level. I fully support the overall goal of the Proposal and hope to see it adopted after some additional considerations.

---

[26] Mutual Fund Directors Forum – Cybersecurity and the evolving threat landscape, DELOITTE DEVELOPMENT LLC; see also Firemen's Ret. Sys. v. Sorenson, No. 2019-0965-LWW, 2021 Del. Ch. LEXIS 234 (Ch. Oct. 5, 2021) (finding that regular board meetings that included a discussion of cybersecurity risks constituted an appropriate following of the "business judgment rule" of decisions made in good faith).

[27] **Proposal** at 13534.

[28] Birdthistle, *Remarks at the ICI Investment Management Conference*, U.S. SECURITIES AND EXCHANGE COMMISSION.

Respectfully submitted,

Trevor H. Fry, Student
Boston College Law School
885 Centre Street
Newton, MA 02469