



MUTUAL FUND DIRECTORS FORUM

The FORUM for FUND INDEPENDENT DIRECTORS

April 11, 2022

Ms. Vanessa Countryman
Secretary
United States Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

Re: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (File No. S7-04-22)

Dear Ms. Countryman:

The Mutual Fund Directors Forum (“the Forum”)¹ welcomes the opportunity to comment on the Commission’s recent rule proposals regarding cybersecurity risk management programs for registered investment companies and investment advisers.² Given the importance to funds and their investors of appropriately managing the cyber risks faced by funds and their service providers, we welcome the Commission’s efforts to provide greater clarity in this area.

The Forum is an independent, non-profit organization for investment company independent directors and is dedicated to improving mutual fund governance by promoting the development of concerned and well-informed independent directors. Through education and other services, the Forum provides its members with opportunities to share ideas, experiences and information concerning critical issues facing investment company independent directors and also serves as an independent vehicle through which Forum members can express their views on matters of concern.

¹ The Forum’s current membership includes over 943 independent directors, representing 123 mutual fund groups. Each member group selects a representative to serve on the Forum’s Steering Committee. This comment letter has been reviewed by the Steering Committee and approved by the Forum’s Board of Directors, although it does not necessarily represent the views of all members in every respect.

² See *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, Release Nos. 33-11028 and IC-34497 (File Nos. S7-04-22), 87 Fed. Reg. 13524 (Mar. 9, 2022) (*hereinafter* “Proposing Release”).

1. Requiring Cybersecurity Programs

Registered funds and their advisers are typically highly dependent on information technology systems to run and manage their businesses on a daily basis – indeed, technology typically pervades every part of a fund’s operations, from portfolio management to compliance to the maintenance of information on the fund’s investors. The reliance on technology brings with it vulnerability to attack by malicious actors. In particular, over at least the last dozen years, cyber risk and the need to have a cybersecurity program have grown in importance for funds and their advisers. During that time, the cyber risk environment has continually changed and become more complex, and as a result the actions that advisers and other entities servicing funds have needed to take to protect their technology infrastructure have also become more substantial, more complex and more expensive.

In short, managing a fund today requires a fund adviser to have a cybersecurity program focused both on its own risks as well as the risks faced by the funds’ third-party service providers. The failure to have an effective program creates significant risks that a fund will not be able to service its shareholders appropriately or continue to comply with its legal and regulatory obligations. Therefore, as the Forum and other industry groups have long recognized, having an appropriate approach to cybersecurity is part of the fiduciary obligation that an adviser owes a fund and its shareholders. As part of the general oversight of a fund’s and adviser’s risk management programs, the directors of a registered fund thus have a correlative fiduciary obligation to oversee the adviser’s cybersecurity program on behalf of a fund’s shareholders. We welcome the Commission’s ongoing attention to the importance of cybersecurity in the fund industry as demonstrated both by its prior work and through this rule proposal.

We generally support the direction that the Commission has taken in the rule. In particular, we agree that advisers and funds should have policies and procedures governing their cybersecurity programs and that fund directors should provide appropriate oversight for these programs. We therefore support, subject to our comments below, the adoption of Rule 38a-2. We believe this rule would result in little change within the industry. Whether characterized as policies and procedures or dealt with under another rubric, the vast majority of advisers to funds already have cybersecurity programs in place and directors similarly recognize the important role they play in overseeing how these plans are structured, implemented and maintained.

Directors also continue to take an avid interest in developments with respect to cybersecurity and their role in overseeing their funds’ cybersecurity programs. On numerous occasions, both in response to the specific interests of our members and as part of our goal to better educate the independent director community, the Forum has published White Papers and other advice for fund directors to help them better understand the risk environment and develop effective approaches for providing oversight for the cybersecurity programs that protect the funds they oversee.³ Later this month, we will publish a further report on cybersecurity for directors, *Cybersecurity and the Evolving Threat Landscape: The Role of the Mutual Fund Director*. We

³ See, e.g., Mutual Fund Directors Forum, *Board Oversight of Cybersecurity* (November 2015). See also, Mutual Fund Directors Forum, *Role of the Mutual Fund Director in the Oversight of the Risk Management Function* (May 2020).

plan to continue to work proactively with the independent director community to help them remain responsive to the evolving cyber risk environment.

Most fundamentally, we agree with the Commission's statement that cybersecurity programs should not be generic, but rather should be tailored to the specific business, needs and technology of the fund to which it applies. Indeed, a cybersecurity plan not tailored in this manner is likely to be ineffective. We believe that the elements that the proposed rule would require cybersecurity policies and procedures to include are consistent with the elements fund directors look for when evaluating cybersecurity plans. In particular, risk assessment, management of user access, the protection of information, threat and vulnerability management and planning for incident response and recovery are clearly important elements of any fund's or adviser's approach to cybersecurity.

We caution the Commission to take care that its enumeration and description of these elements not undermine the importance of every individual fund's cybersecurity program being tailored to its needs. In describing the individual elements, the Commission also suggests various approaches and factors that funds and advisers might consider in developing and updating their cybersecurity programs. While there is nothing inherently problematic about anything identified by the Commission, there is always a risk that examples in a rulemaking release become a checklist, either when firms design their cybersecurity plans or when that plan is assessed as part of a Commission examination. The Commission should consider both the dynamic nature of cybersecurity threats as well as the need to allow every fund and adviser to tailor its program to its own business and own needs in determining whether specific factors should be included in the final release. We also urge the Commission to give appropriate deference to advisers and funds in designing their programs, and not second guess reasonable approaches to cybersecurity that are developed by individual entities.

2. Role of Independent Directors

As we have noted above, directors have a clear fiduciary duty to use their business judgment to provide oversight to the cybersecurity programs connected to the funds for which they are responsible. Broadly, we agree that approving the relevant policies and procedures and reviewing an annual report on the operation of those policies and procedures (including reviewing changes made to the program and any notable cyber events that have occurred in the past year) is appropriate.

More importantly, we think it is of fundamental importance that the Commission recognizes in the Proposing Release that directors "may satisfy their obligation with respect to the initial approval by reviewing summaries of the cybersecurity program prepared by persons who administer the fund's cybersecurity policies and procedures." Effective oversight does not require that directors understand and review every aspect of a cybersecurity program that has been developed by the adviser's technology experts. Indeed, independent directors should not be required to be technology experts. Rather, they need to have a broad-based and high-level understanding of cyber issues combined with the necessary judgment to go beyond "passive" oversight to provide appropriate review and approval of the fund's cybersecurity program. As our

upcoming report will emphasize, directors should, on an ongoing basis, “remain vigilant and ask key questions about the cybersecurity program.” They will be more effective in accomplishing this goal by relying on appropriate summaries rather than having to review and approve every technical aspect of the policies and procedures presented for approval. We encourage the Commission to continue to define the director’s role in this manner.

3. Reporting of Cyber Incidents

In spite of our support for the general approach of the Commission’s proposed rule, we have serious concerns about the proposed requirement that an adviser to a fund report a “significant” cybersecurity event to the Commission within 48 hours.

As the Commission’s proposed rule already recognizes, an appropriate cybersecurity plan will include plans for responding to and recovering from a cyber event. However, no matter how well a cybersecurity plan outlines proposed responses to and means of recovery from a cyber incident (including appropriate reporting chains within the fund adviser and to the fund’s board), the period following a cyber event is likely to be both consuming and rapidly evolving. Once a cyber incident is uncovered, the fund, adviser or other victim of the event will likely be fully engaged in understanding the scope of the event, assessing whether any losses or corruption of data have occurred, determining whether a hacker is still present in its systems, and developing an initial recovery plan appropriate to the incident that has actually occurred. The fund and its adviser will also likely be seeking both outside technical and legal assistance and may be assessing who it needs to inform in the initial instance – anyone ranging from business partners, the fund’s independent directors, fund investors and criminal authorities. These decisions will depend on the adviser’s evolving understanding of a changing situation and what its existing policies and procedures governing reporting on the incident require.

Imposing an obligation on fund advisers to continually assess during this period whether the cyber incident is “significant” – a term that the Commission defines in only the most general terms – can easily become a distraction from the other, more important recovery actions that the adviser is undertaking. Moreover, given the evolving nature of the early stages of recovery from a cyber incident, the task of determining whether the adviser has a “reasonable basis” to conclude a significant cyber event has occurred is an inherently difficult and subjective task. Placing an additional legal liability on an adviser to make this decision – and, as the proposed rule would also require, to update any filing made with the Commission within 48 hours as the situation changes – during the initial hours of its response to a cyber event makes little sense.

In the end, no cybersecurity program is perfect; as with other financial services businesses, advisers’ systems are always at risk of attack and advisers are always responding to the activities of potentially malicious parties. Most cyber incursions and attacks have limited impacts and are clearly not significant. We do recognize that significant cyber events are important, and that the Commission has a legitimate interest in understanding cyber events that have an impact on fund investors and in understanding how the adviser addresses and recovers from them. In the rare instances in which a cyber event may have a broader impact on the financial markets, the Commission has an obvious interest in understanding the incident and working to limit its impact.

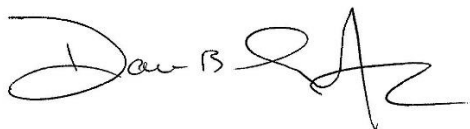
Perhaps most importantly, the fund industry as a whole has an interest in learning from one another and working together to develop effective techniques to prevent and respond to the ever-changing cyber risk environment. The Commission should seek to facilitate this spirit of collaboration. Imposing a very short fuse reporting requirement on advisers seems unlikely to assist the Commission in fulfilling its role and risks undermining the spirit of collaboration that should exist between the Commission and all industry players with respect to cyber attacks. Moreover, advisers with well-designed cybersecurity programs are unlikely to have any interest in preventing the Commission from learning about cyber attacks. We therefore encourage the Commission to reconsider this short fuse reporting requirement and instead develop an approach to information sharing that will foster collaboration in the ongoing industry response to cyber risks.

4. Conclusion

In sum, given the growing importance of cybersecurity, as well as the key role that fund directors play in the oversight of risk management programs, we generally support the Commission mandating that fund advisers have cybersecurity plans and that directors play a role in overseeing them. However, no matter how strong individual cybersecurity plans are, cyber incidents are inevitable. For the reasons outlined above, we believe that the Commission's requirement that advisers report "significant" incidents within 48 hours is not only unnecessary but may also hinder the activities necessary to recover from a cybersecurity incident.

We would welcome the opportunity to discuss these comments in further detail. Please feel free to contact David Smith, the Forum's General Counsel, at David.Smith@mfdf.org or 202-507-4491 or Carolyn McPhillips, the Forum's President, at Carolyn.McPhillips@mfdf.org or 202-507-4493.

Sincerely,

A handwritten signature in black ink that reads "David B. Smith, Jr." followed by a stylized flourish.

David B. Smith, Jr.
Executive Vice President & General Counsel