Managed Funds Association
The Voice of the Global Alternative Investment Industry
Washington, D.C. | New York | Brussels | London

May 22, 2023

Via Electronic Mail: rule-comments@sec.gov

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

Re: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period; File No. S7-04-22

Dear Ms. Countryman,

Managed Funds Association[1] ("**MFA**") welcomes the opportunity to further comment[2] on the proposed rule release from the Securities and Exchange Commission (the "**Commission**"), "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies" (the "**Proposed Rules**").[3]

We initially submitted comments to the Proposed Rules on April 11, 2022.[4] In our prior comment letter, we expressed our support for the objective underlying the Proposed Rules, while also expressing concern about the breadth of certain aspects of them, including the proposed cybersecurity incident notification provisions. Specifically, we stated that the Commission should amend the Proposed Rules to:

- Narrow the definition of "adviser information";

[1] Managed Funds Association ("**MFA**"), based in Washington, D.C., New York, Brussels, and London, represents the global alternative asset management industry. MFA's mission is to advance the ability of alternative asset managers to raise capital, invest, and generate returns for their beneficiaries. MFA advocates on behalf of its membership and convenes stakeholders to address global regulatory, operational, and business issues. MFA has more than 170 member firms, including traditional hedge funds, credit funds, and crossover funds, that collectively manage nearly $2.2 trillion across a diverse group of investment strategies. Member firms help pension plans, university endowments, charitable foundations, and other institutional investors to diversify their investments, manage risk, and generate attractive returns over time.

[2] *See* Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period, 88 Fed. Reg. 16921 (March 21, 2023), available at https://www.govinfo.gov/content/pkg/FR-2023-03-21/pdf/2023-05766.pdf.

[3] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 13524 (Mar. 9, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-03-09/pdf/2022-03145.pdf.

[4] *See* Managed Funds Association, *Comment Letter re Cybersecurity Risk Management, File number S7-04-22* (April 11, 2022), https://www.sec.gov/comments/s7-04-22/s70422-20123280-279547.pdf.

- Provide guidance that advisers can choose to, but are not required to, utilize recognized frameworks for reference when developing their cybersecurity policies and procedures;

- Provide a safe harbor for investment advisers that develop their cybersecurity risk management programs based on certain recognized standards;

- Focus on service providers that provide critical services, permit investment advisers to rely on service providers that have certain types of cybersecurity risk management programs, and reflect the commercial reality that investment advisers often will not have the ability to require service providers to amend their contracts or practices as required by the Proposed Rules;

- Narrow the scope of the incident response and recovery requirements in the Proposed Rules to apply only when there is a data breach that leads to actual harm;

- Remove or clarify language that indicates the Proposed Rules would require investment advisers to adopt cybersecurity risk management programs that go beyond existing practices and standards;

- Clarify that the Proposed Rules do not require one specific approach for investment advisers to address recoverability from significant operational disruption;

- Narrow the scope of adviser policies and procedures designed to satisfy the threat and vulnerability management element;

- Define standards with respect to the Commission's expectations regarding multi-factor authentication;

- Simplify the proposed reporting rule to: (1) provide investment advisers with more flexibility regarding the timing of submitting a notice to the Commission; (2) eliminate the detailed initial reporting requirements to require only a notification to the Commission, and (3) eliminate the requirement to amend an initial notification report;

- Provide a 30-day timeline for investment advisers to disclose significant cybersecurity incidents to investors, to begin upon resolution of the significant cybersecurity incident; and

- Supplement the Proposed Rule to require investment adviser cybersecurity risk management programs to include: (1) training of employees; (2) testing of systems; and (3) monitoring of suspicious activities.

MFA continues to advocate for these improvements to the Proposed Rules and reaffirms the points made in its initial comment letter. This submission focuses on the proposed Form ADV-C requirements which, given the tight notification timelines and burdensome substantive reporting provisions, likely interfere with an investment adviser's efforts to respond to a cybersecurity incident. The Commission has now proposed multiple additional rules and amendments regarding cybersecurity, which would, if adopted as proposed, impose overlapping and inconsistent requirements on MFA members.[5] Under these proposed rules, MFA members would, while responding to a significant cybersecurity incident, be required to divert valuable and limited time and resources from mitigating the cybersecurity event to completing regulatory filings with likely incomplete information. The varying timelines for notification under the various proposed rules may also lead to inconsistent reporting to the Commission given that different information will be known immediately after a firm has experienced an attack, 48 hours after, 72 hours after, and so forth.

While we continue to acknowledge the importance of promoting cybersecurity risk management for investment advisers, the burden that would be imposed by the Proposed Rules, in conjunction with the burdens that would be imposed by the Other Cybersecurity Proposals, is likely to, in fact, detract from investment advisers' ability to effectively respond to cybersecurity risks and incidents.

The Commission should consider the importance of regulatory harmonization, in particular as it relates to cybersecurity incident notification, and amend both the Proposed Rules and Other Cybersecurity Proposals to address this issue. As discussed in more detail below, the Commission should amend the Proposed Rules and Other Cybersecurity Proposals to:

- Harmonize the notification timelines applicable to registrants with other regulatory regimes; and

- Simplify cybersecurity incident notification requirements for entities subject to multiple notification requirements to the Commission.

I. The Burden of Overlapping Notification Requirements

The Proposed Rules and Other Cybersecurity Proposals all include separate and distinct cybersecurity incident notification provisions, each with its own trigger, timeline, and

---

[5] Specifically, the Commission has also proposed Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590 (Mar. 23, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-03-23/pdf/2022-05480.pdf (the "**Proposed Issuers Rules**"); Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Swap-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, 88 Fed. Reg. 20212 (Apr. 5, 2023), available at https://www.govinfo.gov/content/pkg/FR-2023-04-05/pdf/2023-05767.pdf (the "**Proposed BD Rules**"); Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, 88 Fed. Reg. 20616 (Apr. 6, 2023), available at https://www.govinfo.gov/content/pkg/FR-2023-04-06/pdf/2023-05774.pdf (the "**Proposed Reg S-P Amendments**"); and Regulation Systems Compliance and Integrity, 88 Fed. Reg. 23146 (Apr. 14, 2023), available at https://www.govinfo.gov/content/pkg/FR-2023-04-14/pdf/2023-05775.pdf (the "**Proposed Reg SCI Amendments**") (collectively, the "**Other Cybersecurity Proposals**").

notification requirements. In addition to the Commission's proposals, MFA members are already subject to multiple preexisting notification requirements.

Responding to a cybersecurity incident is both time-sensitive and resource-consuming. Incident response requires dedicated, specialized resources. The persons responsible for responding to and remediating the incident will, in many cases, be the same persons required to provide the information required to assess and comply with the proposed notification requirements. Managing both the incident response *and* the incident notifications (particularly those with short notification windows) will be difficult and distract from advisers' primary fiduciary responsibilities to their clients and the need to ensure the ongoing security of a firm's systems and data. The Commission's requirements should recognize and enable advisers to act in accordance with their fiduciary responsibilities rather than, as the Proposed Rules would, work against them.

Consider, for instance, a registered investment adviser with an affiliated broker-dealer and issuer parent who experiences a significant cybersecurity incident. That entity could be subject to three separate notification and disclosure regimes. Under the Proposed Rules and Other Cybersecurity Proposals, the firm would potentially need to:

1. Immediately notify the SEC of the incident in writing;[6]

2. Within 48 hours, file Form ADV-C[7] and, depending on the scope of the affiliated broker-dealer, Form SCIR Part I;[8] and

3. Within four business days of a determination that the incident was material, make an 8-K filing.[9]

This regime of multiple notification obligations is particularly burdensome because precise factual determinations for most cybersecurity incidents are exceedingly difficult within the first several days of the incident. Indeed, at the time of most incidents, the investment adviser typically has little reliable information about the matter and must thereafter race to remediate the matter, while also simultaneously trying to determine its cause, impact, and potential harm. This

---

[6] Proposed BD Rules, proposed 17 CFR § 242.10(c)(1) ("A covered entity must give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.").

[7] Proposed Rules, proposed 17 CFR § 275.204-6(a)(1) (Requiring registered investment advisers to "[r]eport to the Commission any significant adviser cybersecurity incident or significant fund cybersecurity incident, promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that any such incident has occurred or is occurring by filling Form ADV-C electronically").

[8] Proposed BD Rules, proposed 17 CFR § 242.10(c)(2)(i) ("A covered entity must report a significant cybersecurity incident, promptly, but no later than 48 hours, upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring by filing Part I of Form SCIR with the Commission.").

[9] Proposed Issuers Rules, proposed Form 8-K, Instruction B.1 ("A report pursuant to Item 1.05 [Cybersecurity incidents] is to be filed within four business days after the registrant determines that it has experienced a material cybersecurity incident.").

challenge of obtaining accurate information about the incident is particularly acute when a cybersecurity incident involves a deliberate attack by a threat actor seeking to harm the investment adviser. As a result, the information ascertained in the first hours and days of an incident is often subsequently rendered inaccurate or incomplete. Accordingly, investment advisers will likely file initial notifications (on varying timelines, which creates a risk of inconsistent notifications as facts develop) that do not contain meaningful information for the Commission's staff. Moreover, because factual developments evolve quickly in incidents, investment advisers will likely have to submit multiple required amendments to the initial notifications,[10] compounding the compliance burden for an investment adviser that is also trying to restore the integrity of its information systems.

This burden is exacerbated by the fact that the Proposed Rules would require notification of isolated, discrete incidents that do not cause widespread or systemic harm to an investment adviser. The Proposed Rules' definition of a significant cybersecurity incident (that is, one that would trigger notification) includes cybersecurity incidents that lead to the unauthorized access or use of adviser or fund information, where the unauthorized access or use results in, in the case of significant adviser cybersecurity incidents, "(i) Substantial harm to the adviser; or (ii) Substantial harm to a client, or an investor in a private fund, whose information as accessed," and in the case of significant fund cybersecurity incidents, "substantial harm to the fund or to an investor whose information was accessed."[11] This language could be read to imply that a cybersecurity incident that impacts the information of *a single investor* would need to be reported to the Commission.

The triggers are also similar—yet unhelpfully distinct—across the proposed rules. Under both the Proposed Rules and the Proposed BD Rules, the unauthorized access of or use of certain information may constitute a significant cybersecurity incident. Under the Proposed Rules, such an incident is significant "where the unauthorized access or use of such information ***results in***" substantial harm, as discussed above. Under the Proposed BD Rules, however, such an incident is significant "where the unauthorized access or use of such information systems ***results in or is reasonably likely to result in***" substantial harm.[12] These inconsistencies further increase the burden on firms subject to both rules to navigate notification obligations in the midst of a cybersecurity incident.

These notifications would all be in addition to existing obligations that investment advisers have under other potentially applicable regimes, such as state data breach notification laws, regulatory regimes like the New York Department of Financial Services' Cybersecurity Regulation or the EU General Data Protection Regulation, and the Commission's Proposed Reg

[10] The investment adviser would be required to update both Form ADV-C and, as applicable, Form SCIR Part I within 48 hours of a determination that information has become materially inaccurate, the discovery of new material information, the resolution of the incident, or the closure of an internal investigation. Proposed Rules, proposed 17 CFR § 275.204-6(a)(2); proposed BD Rule, proposed 17 CFR § 242.10(c)(2)(ii).

[11] Proposed Rules, proposed 17 CFR §§ 275.204-6(b) (significant adviser cybersecurity incident), 270.38a-2 (significant fund cybersecurity incident).

[12] Proposed BD Rules, proposed 17 CFR § 242.10(a)(10).

S-P and Reg SCI Amendments. Furthermore, the newly adopted amendments to Form PF require large hedge fund advisers to notify the Commission on a "current report" as soon as practicable but no later than 72 hours after "the adviser or reporting fund experiences a 'significant disruption or degradation' of the reporting fund's 'critical operations,' whether as a result of an event at the reporting fund, the large hedge fund adviser, or other service provider to the reporting fund."[13] The Form PF Adopting Release recognizes that a cybersecurity incident could trigger a current report under Form PF and that affected registrants will have to comply with both notification requirements.[14]

These requirements contain different triggers, requests for information, and notification timelines. Managing these notifications would be a burdensome and time-intensive process. Given the tight timelines for notification, updates would most likely be required, which would drain even more resources from critical incident response efforts. This is particularly true because, as drafted, these notifications and updates are triggered by determinations that may be required to be made prior to the conclusion of a cybersecurity incident.

The Commission should consider the fact, too, that these resource constraints cannot be solved by simply hiring more people. Investment advisers require qualified cybersecurity professionals for both responding to the incident and providing information for the proposed notification requirements. In addition to the massive financial burden that hiring an entire cybersecurity team would impose on advisers, the current industry-wide shortage of qualified cybersecurity professionals means that investment advisers are unable to simply hire more people with the requisite expertise.[15] Duplicative reporting requirements would take time away from addressing substantive cybersecurity issues.

II. The Importance of Harmonization

Regulatory harmonization is vital to ensuring registrants' ability to comply with their obligations under federal and state laws as well as to providing meaningful information to regulators and investors when a significant cyber incident occurs. As explained above, the proposed cybersecurity incident notification requirements add to the existing burden of notification requirements for registrants under investment agreements, state data breach notification laws, and other federal and international regulatory regimes. For that reason, consistent with this Administration's emphasis on regulatory harmonization, the Commission should streamline and coordinate the notification regimes of the Proposed Rules and Other Cybersecurity Proposals.

---

[13] Amendments to Form PF to Require Event Reporting for Large Hedge Fund Advisers and Private Equity Fund Advisers and to Amend Reporting Requirements for Large Private Equity Fund Advisers, Investment Advisers Act Release No. IA-6297, p. 42 (May 3, 2023) ("**Form PF Adopting Release**").

[14] *Id.* at 45 ("[W]e acknowledge that there are other government cybersecurity initiatives and our own proposed cybersecurity rulemaking as raised by commenters.").

[15] *See, e.g.*, Cybersecurity Workforce Study, (ISC)^2 (2022), available at https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx (identifying a 26.2% year-over-year increase in the global cybersecurity workforce gap and a 9% year-over-year increase in the U.S. cybersecurity workforce gap).

In March 2023, the Biden-Harris Administration released a National Cybersecurity Strategy (the "**Strategy**"), which emphasized the need for cross-agency coordination on this very point.[16] In support of the Strategy's strategic objective to "Establish Cybersecurity Requirements to Support National Security and Public Safety," the policy states that "[e]ffective regulations minimize the cost and burden of compliance, enabling organizations to invest resources in building resilience and defending their systems and assets."[17] It further cautions that, "[w]here Federal regulations are in conflict, duplicative, or overly burdensome, regulators ***must work together to minimize these harms***."[18] The Strategy recognizes the burden posed by overlapping and inconsistent notification requirements and that this burden undermines improving an entity's cybersecurity posture.

The Financial Stability Board, of which the Commission's Chair, the Honorable Gary Gensler, is a member, has issued "Recommendations to Achieve Greater Convergence in Cyber Incident Reporting" (the "**FSB Report**").[19] The FSB Report acknowledges that "[m]eaningful differences in how different authorities determine their reporting criteria for cyber incidents, use incident information and set their timeframes for reporting an incident pose operational challenges for [financial institutions]."[20] The FSB Report recommends that financial authorities "continue to explore ways to align their [cyber incident reporting] regimes . . . to minimise potential fragmentation and improve interoperability."[21]

Consistent with the Strategy and the FSB Report recommendations, the Commission should weigh and minimize the burden of multiple conflicting and overlapping regulatory regimes on its registrants. The Commission's issuance of the Other Cybersecurity Proposals will create further inconsistencies and duplication in cybersecurity requirements, including for MFA members. As discussed above, the burden on investment advisers to navigate such a complex web of requirements is compounded in the heat of an incident, where they will have to manage multiple notification requirements (some with very short deadlines), while also trying to investigate, contain, and remediate the incident itself. As we expressed in our initial comment letter, and consistent with this Administration's priorities, the Commission should deconflict and harmonize obligations and expectations regarding cybersecurity incident notification. We contend that doing so will result in improved cybersecurity risk management—the ultimate goal of these Proposed Rules.

---

[16] National Cybersecurity Strategy, The White House (March 2023), available at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[17] *Id*. at 9.

[18] *Id*. (emphasis added).

[19] Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report, Financial Stability Board (April 13, 2023), available at https://www.fsb.org/wp-content/uploads/P130423-1.pdf.

[20] *Id*. at 4.

[21] *Id*. at 12.

III. Proposed Solutions

Given the burden of these proposed notification requirements and this Administration's recognition of the importance of harmonization across cybersecurity incident notification requirements, the Commission should clarify, extend, and simplify the notification timelines applicable to registrants.

A. Clarify the Triggers for Notification

As discussed above, the definition of a significant cybersecurity event under the Proposed Rules could potentially require advisers to notify the Commission of relatively minor, and certainly non-significant, cybersecurity incidents. Consider, for example, the scenario in which a firm employee inadvertently sends an email containing a single investor's personal information to the wrong recipient. If that information is then misused in a way that causes substantial harm to that single investor, the firm could be required under the Proposed Rules to notify the Commission of the incident. The Commission should revise its definitions of "significant adviser cybersecurity incident" and "significant fund cybersecurity incident" to clarify that the incidents must have significant impacts to the firm. The misuse of a single investor's personal information following a compromise should not necessarily require notification absent other significant effect.

B. Extended Timeline for Notification

The Commission should adopt a more flexible reporting deadline (*e.g.*, promptly after a cybersecurity incident). If the Commission determines that a specific deadline is appropriate under the Proposed Rules, the Commission should at the very least extend the proposed 48-hour deadline to submit Form ADV-C. In particular, the Commission should extend the deadline to four business days, as contemplated in the Proposed Issuers Rule. Notably, other existing regulatory regimes (such as the New York Department of Financial Services' Cybersecurity Regulation and the EU General Data Protection Regulation) have a 72-hour reporting deadline, so the Commission should, at a minimum, consider extending the deadline to at least 72 hours to align with these existing regimes.

Further, as stated in our initial comment letter, the Commission should eliminate the proposed requirement to amend initial notices. To the extent the Commission maintains that requirement, the Commission should similarly extend the timeline for filing required updates to Form ADV-C.

C. Streamlined Notifications to the Commission

We recommend that the Commission simplify notification requirements for entities subject to multiple notification requirements *to the Commission*.

For example, if a registered investment adviser subject to both the Proposed Rules and the Proposed BD Rules experiences a significant cybersecurity incident, the Commission should amend the proposed requirements to permit the firm to file one omnibus notification. The notification should require the same information and should be allowed to be filed on the same timeline. To the extent those timelines are not in fact coordinated, the single omnibus notification

should be allowed to be filed on the longer of the applicable timelines. The Commission should similarly allow a coordinated approach for material incident updates and final incident reporting.

* * *

We appreciate the opportunity to provide additional comments to the Commission on the Proposed Rules, and we would be pleased to meet with the Commission or its staff to discuss our comments. If the staff has questions or comments, please do not hesitate to contact Joseph Schwartz, Director & Counsel, or the undersigned at (202) 730-2600.

Respectfully submitted,

/s/ Jennifer W. Han

Jennifer W. Han
Executive Vice President
Chief Counsel & Head of Global Regulatory Affairs
Managed Funds Association

cc: The Hon. Gary Gensler, Chairman, Securities and Exchange Commission
The Hon. Hester M. Peirce, Commissioner, Securities and Exchange Commission
The Hon. Caroline A. Crenshaw, Commissioner, Securities and Exchange Commission
The Hon. Mark T. Uyeda, Commissioner, Securities and Exchange Commission
The Hon. Jaime Lizárraga, Commissioner, Securities and Exchange Commission
William Birdthistle, Director, Division of Investment Management, Securities and Exchange Commission