12 E 49th Street, 11th Floor, New York, NY 10017
+[redacted]
[redacted]
aima.org

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

Submitted via email to rule-comments@sec.gov

April 11, 2022

Dear Ms. Countryman,

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

The Alternative Investment Management Association (AIMA)[1] appreciates the opportunity to respond to the U.S. Securities and Exchange Commission (Commission or SEC) on its proposed rule to require registered investment advisers ("advisers") and registered investment companies, including business development companies ("funds") to adopt and implement cybersecurity policies and procedures reasonably designed to address cybersecurity risks (the "Proposing Release").[2]

We would like to state at the outset that the significant number of rule proposals, which have been issued by the Commission in quick succession, has meant that our member firms have been overwhelmed and therefore unable to give each particular rule proposal their necessary and full attention. As a result, we would like to again raise our concerns that, despite our requests[3] to extend

[1] The Alternative Investment Management Association (AIMA) is the global representative of the alternative investment industry, with around 2,100 corporate members in over 60 countries. AIMA's fund manager members collectively manage more than US$2.5 trillion in hedge fund and private credit assets. AIMA draws upon the expertise and diversity of its membership to provide leadership in industry initiatives such as advocacy, policy and regulatory engagement, educational programmes and sound practice guides. AIMA works to raise media and public awareness of the value of the industry. AIMA is committed to developing skills and education standards and is a co-founder of the Chartered Alternative Investment Analyst designation (CAIA) – the first and only specialised educational standard for alternative investment specialists. AIMA is governed by its Council (Board of Directors). For further information, please visit AIMA's website, www.aima.org.

[2] SEC, Proposing Release, Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 FR 13524 (Mar. 9, 2022).

[3] *See,* AIMA Letter to SEC, Extension request of comment periods for File Nos. S7-04-22, S7-05-22, S7-06-22 and S7-08-22 (Mar. 3, 2022).

the comment periods, the Commission's overlapping and serially short comment periods have not provided stakeholders the time to fully analyze, consider and comment on this rule proposal, including the time that it takes to study and analyze the market and economic implications of the proposals and identify possible unintended, negative consequences.

That being said, we acknowledge that the ever-increasing digitalization of finance, the growing interconnectedness across financial institutions and third parties and the increased number of cyber threats bring about the need for advisers and funds to strengthen their resilience against cyberattacks appropriately. We also appreciate that advisers and funds of all sizes need to develop an 'information security culture'. However, we believe that there needs to be clear and coherent proportionality within any future rulemaking in this area. For example, smaller advisers will need to take a risk-based approach to their information security planning in line with their size, available resources and capabilities. The expectation levels of regulators will clearly need to vary depending on the size of the adviser or fund and its associated impact on investors and the wider financial system.

We support the Commission and its staff in their efforts to continue to focus on cybersecurity risks to advisers and their clients, as well as to funds and their investors. Cybersecurity risk management is a critical area of focus for advisers and funds, and many advisers and funds have already taken significant steps to address cybersecurity risks. We also support the Commission in its endeavors to provide helpful cybersecurity guidance to advisers and funds, as well as other market participants, to help them to protect their investors from potential cyberattacks.[4]

Last month, AIMA published the latest edition of its *Guide to Sound Practices for Cybersecurity*.[5] The guide draws on the latest insights from advisers' chief technology officers and chief information security officers, other cybersecurity experts and fund investors regarding cyber risk and resilience in the alternative investment management industry. It aims to set out principles that an adviser should consider when developing a cybersecurity programme as part of its overall compliance and operations. Members of AIMA are able to make use of this sound practice guide to assist them in adopting adequate cybersecurity policies and procedures. Furthermore, this guidance outlines sound practices on many of the points in the Proposing Release which help advisers and funds trying to build robust cybersecurity programs, while also allowing the flexibility for them to tailor their policies and procedures to their particular risks.

Unquestionably, cyber crime is a uniquely challenging threat to the global financial system. We appreciate that cyberattacks are continuing to increase at an alarming rate in terms of their size, frequency and sophistication. However, there has been little evidence of material or significant cyberattacks targeted directly at funds and their advisers. It is therefore important that any new rules designed to address cybersecurity risks in the financial services sector are proportionate and appropriate for the alternative investment management industry. We agree that each fund and adviser must consider the cybersecurity risks unique to their particular circumstances and should

---

4 *See*, *e.g.*, Cybersecurity Risk Alert: Safeguarding Client Accounts against Credential Compromise (Sep. 2020), Cybersecurity Risk Alert: Ransomware Alert (Jul. 2020) and Cybersecurity Risk Alert: Safeguarding Customer Records and Information in Network Storage - Use of Third Party Security Features (May 2019).

5 AIMA, Guide to Sound Practices for Cybersecurity (Mar. 2022).

approach cybersecurity in a strategic manner, aligned with its overall business strategy. As each adviser's use of technology is unique, so is its risk profile. As a result, there is no "one size-fits-all" cybersecurity programme.

We would also argue that in many cases the fiduciary obligations of advisers, existing rules applicable to advisers and funds, the modern technological context and commonly employed sound practices, not to mention other existing rules,[6] already require advisers and funds to implement reasonably designed cybersecurity policies and procedures.

Our members have drawn our attention to a number of concerns with the Proposing Release, which are outlined in detail in the Annex. In particular, our members note that:

1. the 48-hour notification period does not provide sufficient time to conduct a thorough investigation into a potentially significant cyber incident. Accordingly, the proposed notification period should be expanded to 96-hours;

2. greater flexibility is needed on the proposed public disclosure requirements, while reporting to the Commission of any cyber incident should not be publicly disclosed;

3. a narrowing of the scope of the service providers included in the proposed rules could reduce costs for advisers and funds and investors without significantly diminishing the positive effects of the new rule;

4. a more proportionate and appropriate approach is required in a number of areas as there is a real risk that some of the proposed rules could cause some advisers and funds to do a disproportionate amount of work for little or no benefit;

5. the proposed rules could introduce significant cybersecurity oversight responsibilities on funds' boards, while many are still evolving their understanding of the rapidly changing cybersecurity environment and risks;

6. a realistic and reasonable timeframe is required for advisers and funds to implement the new requirements; and

7. despite reasonable efforts, advisers could be penalized as a result of the Commission using its anti-fraud authority for the new rule.

---

[6] *See, e.g.,* Regulation S-P Requires registered broker-dealers, investment companies, and investment advisers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." These policies and procedures must be reasonably designed to, among other things, "[p]rotect against any anticipated threats or hazards to the security or integrity of customer records and information," as well as "[p]rotect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer." The relevant text of Regulation S-P is available at: 17 C.F.R. 248.30. Similarly, Regulation S-ID requires advisers to develop and implement an Identity Theft Prevention Program "designed to detect, prevent, and mitigate identity theft" from customer accounts. The relevant text of Regulation S-ID is available at: 17 CFR 248.201.

We would conclude by re-emphasizing our support for the overarching objectives of the Commission in the Proposing Release. We remain at your disposal to provide any clarification on any of the issues raised in this letter. For further information please contact James Delaney at [redacted].

Yours sincerely,

Jiří Król
Deputy CEO, Global Head of Government Affairs
AIMA

Cc: The Honorable Gary Gensler, Chair
The Honorable Hester M. Peirce, Commissioner
The Honorable Allison Herren Lee, Commissioner
The Honorable Caroline A. Crenshaw, Commissioner

ANNEX

Our members have several concerns with the Proposing Release which are outlined in detail below.

1. The 48-hour notification period does not provide sufficient time to conduct a thorough investigation into a potentially significant cyber incident. Accordingly, the proposed notification period should be expanded to 96-hours

Under proposed Rule 204-6 under the Investment Advisers Act of 1940, as amended ("Advisers Act"), advisers would be required to report "significant cybersecurity incidents" to the Commission on new Form ADV-C, including on behalf of any registered funds and private funds that experience such incidents. The reports would have to be made promptly but in no event later than 48 hours after having a reasonable basis to conclude that a "significant adviser cybersecurity incident" or "significant fund cybersecurity incident" has occurred or is occurring.

We understand that Form ADV-C would include both general and specific questions related to the cybersecurity incident, for example, the nature and scope of the incident as well as whether any disclosure that has been made to any clients and/or investors.

When managing a potentially significant cybersecurity incident, the immediate need is to focus on the cyber threat first to fully determine whether or not it is significant, and the practical steps required to mitigate any risks to any clients and/or investors. This requires personnel with the appropriate expertise to assess the incident and as a result of the "all hands-on deck" type situation, the "in no event later than 48 hours" reporting requirement does not provide sufficient time to gather, analyze and understand the information, scope, impact, materiality, etc. of the cybersecurity incident and to prepare a full and informative report to the Commission. Finding the correct balance in responding to perceived cybersecurity threats while protecting investors is a real challenge. The potential consequences of "under-reacting" or "over-reacting" to such threats could be significant, and both risks need to be carefully considered during the assessment stage. The majority of ransomware attacks happen outside of work hours or on weekends or holidays.[7] This is, of course, deliberate by the cyber attackers. While the security teams will be working on incidents immediately, the rest of the business will have even less time to discuss, review and act.

Resources will be constrained so soon after a potential breach, making the 48-hour requirement all the more challenging to meet and therefore, we believe that consistency with other similar regulations would be preferable. For example, the *Strengthening American Cybersecurity Act of 2022* recently signed into law requires that companies in "critical infrastructure sectors" report cyberattacks to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours.[8] While the SEC's proposed new cybersecurity rules for public companies requires the registrant

---

7 *See, e.g.,* https://vision.fireeye.com/editions/07/07-breaking-in-after-hours.html.

8 https://www.congress.gov/bill/117th-congress/senate-bill/3600/text?r=3&s=2#toc-id1E3C7124ACBA4C4986D04F51AD1E8045.

to disclose a material cybersecurity incident within four business days after the registrant determines that it has experienced a material cybersecurity incident.[9]

We believe that a longer notification period of 96 hours seems rational in this instance as, for example, it is unlikely a fund or adviser is as significant or as heavily resourced as those in "critical infrastructure sectors". Critical attention and resource should not be diverted away from appropriate management and response to the cybersecurity incident and an adviser's or a fund's initial focus should be on protecting its clients and investors. Moreover, making it clear exactly when updates are required is important. The first week after an incident could have developments every day — is that a new filing? We believe it is more appropriate to ask for a "discovery" and "resolution" filing requirement. Relatedly, the number of fields in Form ADV-C to which a response would be required is particularly onerous – 16 different items is a considerable number while dealing with a potentially significant incident.

More broadly, if the goal is systemic awareness of market health, then the Commission should rely on agencies (e.g., Treasury, CISA) that are better prepared to do that given their broader scope and the expertise they already have in-house.

2. Greater flexibility is needed on the proposed public disclosure requirements, while reporting to the Commission of any cyber incident should not be publicly disclosed

Under proposed rule 204-6 and amendments to Form ADV Part 2A, as well as amendments to funds' disclosure requirements, advisers and funds would have to report any significant cybersecurity incidents to the Commission and make appropriate disclosures to their clients and investors.

Proposed amendments to part 2A for Form ADV and proposed amendments to fund registration statements would require a narrative description of the cybersecurity risks advisers' face, how they assess, prioritize and address cybersecurity risks and any significant adviser or fund cybersecurity incidents that had occurred in the past two years.

Under the proposed amendments, significant cybersecurity incidents would need to be disclosed either by filing an amendment to Form ADV "promptly" (in the case of advisers) or by amending a prospectus by filing a supplement with the Commission (in the case of funds).

We believe that the Form ADV Part 2A cybersecurity disclosures should not be required until 30 days after resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident. This would allow sufficient time for proper review and analysis of the incident to ensure the facts and circumstances are appropriately reported to the public.

We would also emphasize that if delaying disclosure about a significant cybersecurity incident could increase the chances of recovery of stolen funds or the detection of the wrongdoers in the opinion of law enforcement agencies, the Commission should consider whether temporary relief from its disclosure requirements would best protect investors and the wider financial system.

---

9 https://www.sec.gov/rules/proposed/2022/33-11038.pdf

Moreover, publicly disclosing a breach or payout will likely encourage other ransomware gangs to target the victim again, particularly when knowing that a business will pay ransom. It is known that ransomware gangs have a tendency to retarget their own victims, there is no reason to believe that peer ransomware gangs would not capitalize on any public disclosures.[10]

Separately but relatedly, we believe also that the Commission should not require public disclosure of a fund's or adviser's cybersecurity incidents, i.e., any of the information disclosed on Form ADV-C. We are concerned that unintended release of such details could facilitate future cyberattacks against funds and advisers as well as against advisers and fund with similar systems or vulnerabilities. We also believe that insurance status should be considered sensitive given it is known cyber attackers have targeted firms that are known to be insured or the insurers themselves.[11]

3. A narrowing of the scope of the service providers included in the proposed rules could reduce costs for advisers and funds and investors without significantly diminishing the positive effects of the new rule

The proposed rules require advisers and funds to consider the cybersecurity risks resulting from their reliance on third-party service providers that receive, maintain or process adviser or fund information, or are otherwise permitted to access their information systems and any information residing therein.[12] These requirements would affect a broad range of service providers: not only entities such as custodians, brokers and valuation services, but also email providers, customer relationship management systems, cloud applications and other technology vendors that meet this criterion.

Advisers and funds would be required to document that such service providers implement and maintain appropriate measures to protect information of clients and investors and the systems hosting said information, pursuant to a written contract between the adviser or fund and its respective service provider. This could require advisers and funds to amend numerous existing contracts to modernize or add terms relating to cybersecurity, information protection and business continuity and could potentially extend liability for service provider cybersecurity incidents to advisers and funds that have not adequately engaged in this required oversight. These costs will have to be passed on ultimately to investors.

It is possible that some funds and advisers may find that some of their existing service providers may not be able to enter into suitable written contracts. In this case, the fund or adviser would be required to switch service providers and bear the associated switching costs. In other cases, a fund or adviser may determine that a service provider can be used subject to renegotiation of service agreements, potentially imposing substantial contracting costs on the parties.

The aforementioned costs would be particularly acute for smaller advisers and funds that rely on generic service providers. Smaller registrants may not have sufficient bargaining power with service

---

[10] *See, e.g.,* www.zdnet.com/article/most-firms-face-second-ransomware-attack-after-paying-off-first/.

[11] *See, e.g.,* https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/.

[12] *See* proposed rules 206(4)-9 and 38a-2.

providers of more generic services to effect meaningful changes in cybersecurity practices or contractual provisions.

We would recommend narrowing the scope of service providers covered by the rules to exclude those that present little risk to the fund or adviser as well as those whose cybersecurity practices are already subject to regulatory oversight.

4. A more proportionate and appropriate approach is required in a number of areas as there is a real risk that some of the proposed rules could cause some advisers and funds to do a disproportionate amount of work for little or no benefit

We acknowledge that advisers and funds, regardless of their size, should ensure that the critical and most basic technological defences and practices are in place. Advisers and funds who have considered the extent of cyber-related risks in their operations will know that there is not a "one-size fits all" solution to this threat. The preparation and response must be appropriate to that adviser or fund and proportionate to its size and available resources.

The size, nature and complexity of an adviser's or fund's operations and investment strategy may mean that some of the proposed rules or amendments are in fact disproportionate and inappropriate. There is a need for clear definitions of standards otherwise any ambiguity could lead to confusion and unnecessary costs. In response to the Commission's question, we do not believe that advisers and funds should be mandated to have their cybersecurity policies and procedures periodically audited by an independent third party to assess their design and effectiveness. In many instances, larger advisers will have internal teams who can conduct the annual review. In addition, there is not always a need for third parties for many simple housekeeping security processes, but advisers and funds without internal IT resources may need external support or to be trained on how they can help themselves.

In our view, there is a real risk that the proposed rules and amendments would cause some advisers and funds to do a disproportionate amount of work for little or no benefit. For example, penetration tests are costly and not always the best allocation of a limited information security budget. By doing basic things well, advisers and funds can mitigate many of the threats that they face. We believe that if the Commission were to set requirements to perform penetration testing, for example, this should include flexibility and proportionality in order to address specific needs of advisers and funds by virtue of their size, complexity and scale of operations.

We believe that in some instances the rules might be burdensome for small funds. It might be preferable to reference an existing standard, such as the NIST Cybersecurity Framework,[13] and clarify that a tailoring or "fit for purpose" principle is applied.

For example, in the European Union, the Council (EU-27 Member States) position on the European Commission's legislative proposal for a regulation on Digital Operational Resilience in the EU financial

[13] NIST Cybersecurity Framework is a set of guidelines for mitigating organizational cybersecurity risks, published by the US National Institute of Standards and Technology (NIST) based on existing standards, guidelines, and practices.

services[14] carves out sub-threshold alternative investment fund managers ("AIFMs")[15] and perhaps the Commission could consider introducing a similar exemption or allow for more limited cybersecurity policies and procedures for advisers or funds with assets under management below a certain threshold or with only a limited number of clients or investors.

5. The proposed rules introduce significant cybersecurity oversight responsibilities on funds' boards, while many are still evolving their understanding of the rapidly changing cybersecurity environment and risks

Proposed rule 38a-2 would require a fund's board of directors, including a majority of its independent directors, initially to approve the fund's cybersecurity policies and procedures, as well as to review the written report on cybersecurity incidents and material changes to the fund's cybersecurity policies and procedures. We appreciate that many of these requirements would be consistent with a funds' board's duty to oversee other aspects of the management and operations of a fund.[16]

However, we believe that funds' boards should not be required to approve the cybersecurity policies and procedures of certain funds' service providers, such as advisers, principal underwriters, administrators or transfer agents, and oversee the registered fund's risk assessments of service providers would impose new and significant oversight responsibilities. In practice this would be very difficult to implement.

We would stress that funds' boards are still evolving their understanding of the rapidly changing cybersecurity risks to ensure they can be as effective as possible when it comes to cybersecurity. We acknowledge that funds' boards do not need to be technical experts, but they need to know enough about cybersecurity to be able to have a fluent conversation with their experts and understand the right challenge to ask. We believe the Commission could provide better guidance to funds' boards regarding their initial approval of the cybersecurity policies and procedures, such as additional guidance on documentation provided to the board with respect to the initial approval.

Finally, the Proposing Release does not reference the standard of review that would apply for the various proposed board considerations, such as whether the business judgment rule would apply.

6. A realistic and reasonable timeframe is required for advisers and funds to implement the new requirements

We do not have detailed information on the direct costs linked to the update/review of the existing procedural and organizational arrangements, direct initial and ongoing IT costs or the direct relevant organizational and HR costs linked to the implementation of these rules, however we would strongly encourage the Commission to factor in the additional resources and time that will likely be required for advisers and funds to comply with these new rules and amendments. For example, this might

---

14 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595.

15 To qualify as a sub-threshold AIFM a manager must manage leveraged assets valued at less than €100m or manage unleveraged and closed-ended assets valued at less than €500m.

16 *See, e.g.,* rule 38a-1 under the Investment Company Act; Compliance Program Release, Compliance Programs of Investment Companies and Investment Advisers, SEC Rel. No. IA-2204 (Dec. 17, 2003) [68 FR 74714 (Dec. 24, 2003)], at n.31.

include updating an adviser's digital infrastructure as well as training existing staff or hiring new additional staff. We would therefore encourage the Commission to introduce a 24-36 month compliance period or a tiered timeframe for different requirements to better facilitate and ensure an effective and orderly implementation of the new requirements.

7. Despite reasonable efforts, advisers could be penalized as a result of the Commission using its anti-fraud authority for the cybersecurity rule

In addition to our specific comments above, we would reiterate Commissioner Hester M. Peirce's concerns raised in her statement following the publication of the Proposing Release[17] regarding the imposition of these requirements under Section 206 of the Advisers Act.

Proposed new Rule 206(4)-9 under the Advisers Act would require advisers to registered funds, separately managed accounts and private funds to adopt and implement policies and procedures "reasonably designed" to address cybersecurity risks. However, grounding the proposed new rule in Section 206, the Advisers Act's anti-fraud provision, would mean that not having "reasonably designed" cybersecurity policies is a fraudulent, deceptive, or manipulative act, practice or course of business within the meaning of section 206(4) of the Advisers Act.

Given the prevalence of cyberattacks and the likelihood that cyberattackers will be ever more determined and creative, there is a real risk that the prescriptive cybersecurity rules could become an easy hook for an enforcement action, even when an adviser has made efforts to comply that were considered reasonable before the new threat vectors made that seem unreasonable. As noted by the Commission in the Proposing Release, *"Even when cybersecurity preparations are high, a cybersecurity attack may succeed."*

Based on the facts and circumstances as they existed at the moment it could be reasonable for some advisers to not engage in certain cyber resilience measures, for example, due to its size and impact, but in hindsight after the incident those measures might have prevented a successful cyberattack from occurring.

We would instead support the Commission using an alternative authority, such as its general rulemaking authority in section 211 of the Advisers Act.

[17] https://www.sec.gov/news/statement/peirce-statement-cybersecurity-risk-management-020922.