May 22, 2023

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

Via email to rule-comments@sec.gov

RE: Proposed Rule: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period
File Number S7-04-22

Dear Ms. Countryman:

Thank you for the opportunity to comment on the Commission's proposed rule regarding cybersecurity risk management for certain regulated entities. As cybersecurity consultants that focus exclusively on Registered Investment Advisers ("RIAs"), we are encouraged to see the Commission's focus on cybersecurity with the goal of reducing the overall risk level across such entities that are unquestionably high value targets for threat actors.

Our work consists primarily of serving small and mid-sized RIAs in the cybersecurity arena, and thus our comments are focused specifically on the impact of the proposed rules related to our past and ongoing work with that size of organization. Our organization spans compliance and cybersecurity disciplines with both Certified Ethical Hacker as well as Investment Adviser Certified Compliance Professional® designations held by our professionals.

Overall, we are supportive of the Commission's goals with the proposed rules: namely to lower the cybersecurity risk of regulated entities while also supporting greater transparency with the investing public when choosing a firm to place their trust in. The Commission observes that "*certain advisers and funds show a lack of cybersecurity preparedness, which puts clients and investors at risk*", a conclusion that is supported by our experience among small and mid-sized RIAs. While the largest RIAs have greater resources to enable them to arrive at a more accurate understanding of cybersecurity risk, small and mid-sized RIAs often don't have the in-house expertise to appropriately evaluate cybersecurity risk, and thus unintentionally end up with far greater risk exposure than they realize.

While we certainly understand the viewpoint of many commenters that the proposed rules (especially when considered in totality with the number of proposed rules the Commission has published over the past 18 months in this area) can create undue burden on RIAs and other regulated entities, we are hopeful that the final rule will provide well defined guidelines which make clear for small and mid-sized RIAs exactly what is required (and appropriate) to achieve an acceptable level of cybersecurity risk. We also encourage the Commission to consider areas many commenters in common (ourselves included) have pointed out as being inappropriate, overly burdensome, or unreasonable. We are hopeful our comments provide specific feedback for the Commission to consider in both areas.

ADVISER CYBER

7310 North 16th Street, Suite 130
Phoenix, AZ 85020
602-297-2400
www.advisercyber.com

We begin with the proposed Rule 204-6 which would mandate disclosure on Form ADV-C within "*48 hours after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident occurred or is occurring*". We feel Commissioner Peirce's statement[1] on reporting requirements very effectively articulates many of the potential flaws with this proposed rule but wanted to supplement with our own 'in the trenches' perspective.

Having navigated clients through events that would be a 'significant adviser cybersecurity incident' as defined in the proposed rules, our experience is that 48 hours is far too short of a period for any reasonable conclusions to be drawn or to have any substantive information to report. Often, it takes much longer than 48 hours to engage a cybersecurity insurance carrier, legal counsel, and incident response team and understand the full scope of the incident as well as form a plan to deal with the incident. Quite frequently, negotiations with threat actors (which may be required in the case of ransom demands) are ongoing past the initial 48 hours and thus would be unsettled at the time the initial reporting requirement is triggered.

Additionally, our experience is that it often takes the engaged incident response team days or even weeks or months to fully understand the scope of the attack, which would also be required to report any meaningful data to any regulating entity. In much larger organizations the resources exist to dedicate solely to meeting any proposed reporting requirements (although the arguments regarding the timeline above would nonetheless apply even in the largest organizations). In small and mid-sized RIAs, however, the reporting requirements as proposed would take critical resources away from key initial goals of any incident response: stopping the threat, business continuity, and recovery.

Even if those resource constraints did not exist in small and mid-sized RIAs, the value of any information provided to the Commission on such a short timeframe would be minimal at best, especially since the Commission's core focus is not the intake, interpretation, and determination of appropriate response from information gained from a cybersecurity incident at a regulated entity. As other commenters have pointed out, there are other federal agencies which do have such capability, such as the Federal Bureau of Investigation and the Cybersecurity & Infrastructure Security Agency. With the latter specifically, mechanisms are already in place to ingest data related to cybersecurity incidents, interpret it appropriately, and quickly disseminate notification to the public or to specific industries in the form of advisories.

We would respectfully encourage the Commission to consider a more reasonable timeframe for any reporting requirement and would also encourage the consideration of working with existing federal agencies and resources better suited to handle this type of information. The Commission could certainly continue to utilize its existing mechanisms such as periodic Risk Alerts to enhance and place focus on any observed trends across the industry.

We would also agree with other commenters that have pointed out that even if information regarding cybersecurity incidents were submitted to the Commission and then disseminated to the public via form ADV-C or some other mechanism, the usefulness of such information would be so low that it may be more detrimental than beneficial. There is a saying in the cybersecurity realm that there are only two types of organizations: those that have been hacked and know it and those that have been hacked and simply don't know it yet. The implication is that just because an organization is not aware of a significant

[1] https://www.sec.gov/news/statement/peirce-statement-enhanced-cybersecurity-031523

cybersecurity incident does not mean one has not occurred. To give the investing public the impression that an RIA who has not disclosed a cybersecurity incident on their form ADV-C is somehow indicative that they have never been the victim of such an incident is at best simply not accurate and at worst misleading information from a trusted regulator.

The argument could made that an RIA who has experienced a cybersecurity incident presents a lower risk to the investing public because they have likely taken significant risk mitigation steps in the aftermath of an attack – something which may be counterintuitive to the public and thus disclosure of an attack may create unnecessary confusion. Also as other commenters have pointed out (specifically those from the cybersecurity discipline), ANY public dissemination of information of any type related to a cyberattack would be rich data for threat actors to leverage either while the attack is ongoing (imagine a threat actor involved in ransom negotiations with a victim who has the benefit of reading all of the public disclosures potentially as often as every 48 hours), or to launch additional attacks in the future.

Finally, as demonstrated by various enforcement actions over the past several years[2], the Commission's Division of Enforcement remains vigilant in investigating and taking action against RIAs who are not following appropriate standards related to cybersecurity. Any investor performing due diligence when considering whether to work with a particular firm would certainly review any enforcement actions against that firm. Such action represents far more useful information to the investing public that is attempting to draw a conclusion based on the disclosure of a cybersecurity incident. If a violation results in action by the Division of Enforcement, it can be assumed it was significant and should be considered in evaluating a firm.

Taken together these factors related to the proposed disclosure requirements in rule 204-6 work directly in conflict with the Commission's goals of lowering risk, protecting the investing public, and not placing undue burden on regulated entities. We would encourage the Commission to consider significant restructuring of these requirements towards the following characteristics:

1. Significantly restructure the timeline of any required disclosures. At the very minimum the reporting requirement should not be less than 30 days, and more reasonably 30-90 days after discovery and confirmation a significant cybersecurity incident has occurred.
2. Consider leveraging existing reporting mechanisms already in place with other federal agencies and create a partnership with those agencies to allow the Commission to evaluate macro industry trends that would be appropriate to address with a Risk Alert or other similar mechanism.
3. Carefully consider the confidentiality and protection of information submitted to any federal body. This could include:
    a. Alternate mechanisms of submission (telephone)
    b. Removing any identifiable information associated with any report (effectively allowing anonymous reporting)

[2] Several recent examples include Administrative Proceedings against Cetera Entities https://www.sec.gov/litigation/admin/2021/34-92800.pdf, Cambridge https://www.sec.gov/litigation/admin/2021/34-92806.pdf, and KMS Financial Services, Inc. https://www.sec.gov/litigation/admin/2021/34-92807.pdf.

c. Forgoing reporting requirements altogether since the information is of limited use by the investing public and confidentiality and protection of any submitted information cannot be ensured.

Our review of the proposed rules also resulted in a number of elements which are not explicitly required; however, we believe they are a critical part of achieving an appropriate level of cybersecurity risk and also relatively inexpensive to implement and manage with widely available technology even in small and mid-sized RIAs. Specifically, Section II(1)(b) calls out the following using phrases such as "should", "could" or "may" consider. We would encourage the Commission to modify this language to require these elements instead:

1. Detection security capabilities that can identify threats on a network's endpoints – ideally the final rule would specifically call out not only malware detection/prevention capabilities on endpoints, but also endpoint detection and response capabilities.
2. Role specific cybersecurity threat and vulnerability and response training.
3. Measures reasonably designed to identify suspicious behavior that include consistent monitoring of systems and personnel.
4. Rules to identify and block the transmission of sensitive data.
5. Implementing a patch management program.
6. Backing up data.
7. Incident response plan testing.

By contrast, there are also elements of the proposed rules which use many of the same conditional terms called out above which we believe should remain conditional for small and mid-sized advisers specifically due to the overly burdensome and unreasonable costs and/or complexity associated with incorporating them into a firm's overall compliance program. That isn't to say we don't consider these elements important, rather it is an acknowledgement of the limited resources available to small and mid-sized RIAs and thus the need to prioritize elements designed to mitigate cybersecurity risk. The conditional language certainly encourages firms to consider these elements, but does not make it an explicit requirement:

1. Penetration testing, although if a penetration test is conducted, we support the requirement to track actions taken in response to findings.
2. Mobile device manager
3. Non-SMS based Multi-Factor Authentication

The Commission also asked for feedback in the draft regulation regarding whether additional or more specific requirements should be included. We believe the regulations would be enhanced with the following:

1. Adding the requirement to align with a framework. The Commission has specifically called out the NIST Cybersecurity Framework in the past[3], and there are several commercially available frameworks as well[4]. The specific framework isn't as important as being explicit that alignment with a framework is required since that makes it clear to registrants what they must do to be compliant versus more abstract guidance that exists today.

[3] See Endnote 13 at https://www.sec.gov/investment/im-guidance-2015-02.pdf
[4] https://www.cisecurity.org/controls is one such example

ADVISER CYBER

7310 North 16th Street, Suite 130
Phoenix, AZ 85020
602-297-2400
www.advisercyber.com

2. Given that Business Email Compromise is often cited as one of if not the most common attack vectors today, the Commission should consider adding a requirement for protection technology specifically designed to combat those attacks which includes:
    a. URL rewriting and inspection with automatic malicious URL blocking
    b. Email gateway malware inspection with rejection or at a minimum quarantining of positive results with admin approval for release from quarantine
    c. Sandboxing, detonation, or other safe-file conversion to protect against weaponized attachments
    d. Email impersonation attack detection
3. The Commission should specifically call out a requirement for Security Incident and Event Monitoring (SIEM), Intrusion Detection System/Intrusion Prevention System (IDS/IPS), or other real time monitoring tools. Limiting damage from a significant cybersecurity incident requires extremely rapid response and time sensitivity. Ensuring indicators of an incident are captured in real time and routed to appropriate resources that can respond appropriately is critical to mitigate risk.
4. The final rule should include a requirement to remediate high risk items identified or called out by the various cybersecurity technologies being implemented. There are many tools available on the market today which will detect vulnerabilities or other cybersecurity issues requiring attention and report on the existence of those items, however if those items are not evaluated and incorporated into a remediation plan the efficacy of the alert is severely limited.

We thank the Commission for their work in lowering the level of cybersecurity risk among regulated entities and recognize this is no easy task given the broad scope of organization types that fall within the Commission's jurisdiction. We are hopeful our comments prove meaningful in the consideration of final regulations. We look forward to the final release and working in partnership with industry members to comply with the final regulations in a way which aligns with the resources available in small and mid-sized RIAs.

Sincerely,

/s/

Michael W. Cocanower
Chief Executive Officer