RECHTMAN CPA PLLC
1646 Federspiel Street
Fort Lee, NJ 07024
(917) 566-0020
www.rechtman.com

February 24, 2022

To:
Secretary, Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090
Via Email: *rule-comments@sec.gov*

Re: **Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies**

File Number: **S7-04-22**

To whom it may concern:

In response to the Proposed Rule on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, File Number S7-04-22 (the "Proposed Rule") Rechtman CPA PLLC is pleased to provide our comments to the Securities and Exchange Commission in furtherance of creating an effective cybersecurity rule.

EXECUTIVE SUMMARY

The Proposed Rule, while containing certain helpful requirements such as a mandatory risk assessment, consideration of access controls, a periodic review of compliance and risk, and disclosures of incidents is also fraught with deficiencies. These deficiencies may create an additional burden and elevated risk to Registered Investment Adviser ("Adviser"):

- **The public disclosure of the nature of risks could provide a roadmap to hackers** and to rogue players in further breaching into the environment of reporting Adviser; This is a very significant elevation of risk that should be abated by making the reporting *confidential* and thus – not public. The idea that investors, now informed of such breaches will adjust their expectations based on reported incidents and breaches is well intentioned, but it ignores the reality that any technical information could be used against the reporting Adviser. It is our view that **reporting of breaches or incidents should go only to the Fund Board, except as a confidential reporting to the FBI or other governmental agencies for the purpose of technical analysis.**

- **There is no delineation, between "incident" and "breach"**. Such a differentiation and definition already appear in other Federal laws such as HIPAA and should be re-applied in this here Proposed Rule. The absence of clear definitions creates vagueness in the Proposed Rule and even makes compliance impractical, especially in light of the 48 hours reporting deadline. Establishing a definition that differentiate between "incident" and "breach" would be helpful.

- **The Proposed Rule lacks a singular standard of performance and evaluation**. Such standards exist in other governmental rules. For example, the National Institute for Standards and Technology ("NIST") has an excellent cybersecurity standard. The Proposed Rule will be enhanced in it will have a NIST-based cybersecurity standard.

- There is **over prescription** of controls to be put in place. Back in 1996, when HIPAA was enacted "anti-virus" was all the rage, and it found its way to a law. Nowadays it is less relevant. Similarly, multi-factor authentication is now "all the rage", so it is understandable that it is included in the Proposed Rule. Instead, such technological controls be left the more agile and flexible risk assessment process and the iterative results of re-assessment. R**egulators should leave the technological responses to a Board monitored risk assessment and risk management process that is best suited to determine the technological responses to the assessed risks.**

- **More frequent reviews should be mandated rather than annually.** The requirement for an annual review may appear reasonable for financial performance, but when it comes to cybersecurity risks, such reviews should occur more frequently, *and also* after each breach.

ABOUT RECHTMAN CPA PLLC

Rechtman CPA PLLC™ provide services in fraud investigation, forensic accounting, information technology, data mining, and computer aided auditing,

Our specialty with these services includes fraud investigation for asset misappropriation, litigation consulting, HIPAA and healthcare compliance, civil, damages, insurance claims, evaluation of internal controls, risk analysis, information systems, information technology, Service Organization's Controls (SOC) under SSAE, and SOX 404A testing. We also provide tax compliance services, with a specialty in clergy-related tax matters.

Our experience is in a wide range of industries such as construction, healthcare, real estate, construction, hospitality and dining, professional services, not-for-profit, technology, closely held companies, ERISA plans, and education.

We are pleased to present our detailed analysis in the following pages. With any questions, please contact the undersigned.

Sincerely,

Yigal M. Rechtman, CPA, CFE, CITP, CISM
Managing Member

DETAILED ANALYSIS OF THE PROPOSED RULE

#	***Citation*** **followed by Proposed rule topic**	**Our Comment**
1	*I. Introduction (A) Adviser and Fund Cybersecurity Risks:* "At the same time, cyber threat actors have grown more sophisticated and may target advisers and funds, putting them at risk of suffering significant financial, operational, legal, and reputational harm"	This is an appropriate risk as identified by the Proposed Rule.
2	*I. Introduction (B) Current Legal and Regulatory Framework:* "As fiduciaries, advisers are required to act in the best interest of their clients at all times"	We agree with the fiduciary role of Advisers.
3	*I. Introduction (C) Overview of Rule Proposal* "..which would require advisers and funds that are registered or required to be registered with us to implement cybersecurity policies and procedures addressing a number of elements"	Risk management Policies and procedures for cybersecurity are in all likelihood already in place for most Advisers. Advisers are not just "sitting around" waiting for an incident or a breach. As such, while the introduction is helpful for a foundation, it breaks no new grounds.

#	***Citation* followed by Proposed rule topic**	**Our Comment**
4	*II. Discussion (A) Cybersecurity Risk Management Policies and Procedures* "As discussed below, while the proposed cybersecurity risk management rules would require all such advisers and funds to implement cybersecurity hygiene and protection measures, we **recognize that there is not a one-size-fits-all approach to addressing cybersecurity risks**"	This recognition is false. While "one size" does not "fit all" when it comes to attire, the risk of breaching an Adviser's system is twofold: a. These systems are a treasure trove of confidential information could be gained from accessing an Adviser's system. b. The Adviser may be a vendor to other, larger organizations and as such their system may be a conduit to larger data sets of confidential information. This is a pervasive risk because the weakest link in a chain of electronic trust is the link most likely to be breached. So the small, simple environment of one Adviser is as important as that of a large, complex environment of another Adviser.
5	*II. Discussion (A) Cybersecurity Risk Management Policies and Procedures* "(1) We request comment on the entities subject to the proposed rules: Should the Proposed Rule exempt certain types of advisers or funds from these proposed cybersecurity risk management rules? If so, which ones, and why?"	The exemption is not for the reporting itself but for such a report to being disclosed to the public, as it may give other bad actors a road map to the security, policies, and procedures of the Adviser. Disclosures should be made in coordination with organizations such as the FBI's National Cyber Investigative Joint Task Force ("NCIJTF") and perhaps the U.S. Whitehouse executive offices on cybersecurity.
6	*II. Discussion (A) Cybersecurity Risk Management Policies and Procedures* "(2) Should we scale the proposed requirements based on the size of the adviser or fund?	There should be no scale for risk, for the same reasons we described in responding to II(A), [see item #5 above].

#	***Citation* followed by Proposed rule topic**	**Our Comment**
7	*II. Discussion, (A) Cybersecurity Risk Management Policies and Procedures (1) Cybersecurity Risk Management Policies and Procedures* "The proposed cybersecurity risk management rules would require advisers and funds to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks"	A risk management program is most likely already in place. There are other regulations that may require it (for example, NYCRR 500), as well as best practices mandate. There should be room in the Proposed Rule to rely on existing Risk Assessment and not "re-invent the wheel" when it comes to regulations. For example, an Advisor with an existing NIST based risk assessment under NIST Standard 800-30 should suffice as a repurposed risk assessment. The Proposed Rule should be explicit about this allowance.
8	*II. Discussion, (A) Cybersecurity Risk Management Policies and Procedures (1) Required Elements of Advisers' and Funds' Policies and Procedures* "The proposed cybersecurity risk management rules also would provide flexibility for the adviser and fund to determine the person or group of people who implement and oversee the effectiveness of its cybersecurity policies and procedures"	While this statement is correct, it does not somehow "alleviate" the burden of the Adviser and does not address the risks of exposing the aforementioned road map (see #5 above).

#	***Citation* followed by Proposed rule topic**	**Our Comment**
9	*II. (A) Cybersecurity Risk Management Policies and Procedures (1) Required Elements of Advisers' and Funds' Policies and Procedures (a) Required Elements of Advisers' and Funds' Policies and Procedures* "The first step in designing effective cybersecurity policies and procedures is assessing and understanding the cybersecurity risks facing an adviser or a fund" and "The proposed rules would also require written documentation of any risk assessment"	This is a useful, reasonable requirement. A risk assessment makes a lot of sense for all sorts of purposes, and may already be required, for example: • Health Information Portability and Accountability Act ("HIPAA"), • U.S. Department of Labor Employee Benefit Security Administration, and • Management of Health and Safety at Work Regulations. • Cybersecurity Requirements for Financial Services Companies, New York State, NYCRR Part 500 • Standards for The Protection of Personal Information of Residents of the Commonwealth of Massachusetts, 201 CMR 17.00. Stating that it must be documented is imperative.
10	*II. Discussion, (A) Cybersecurity Risk Management Policies and Procedures (1) Required Elements of Advisers' and Funds' Policies and Procedures (b) User Security and Access* "As an element of an adviser's or fund's reasonably designed policies and procedures, the proposed cybersecurity risk management rules would require controls designed to minimize user-related risks and prevent the unauthorized access to information and systems"	While correct, this requirement is going to be addressed by the risk assessment. Requiring it is an imperative, but simply makes the proposed rule lengthy for no reason. Any reasonable risk assessment will include "user security", "authentication", and "authorization" risks and risk management controls.

#	***Citation* followed by Proposed rule topic**	**Our Comment**
11	*II. Discussion, (A) Cybersecurity Risk Management Policies and Procedures (1) Required Elements of Advisers' and Funds' Policies and Procedures (c)Information Protection* "As an element of an adviser's or fund's reasonably designed policies and procedures, the proposed cybersecurity risk management rules would require advisers and funds to monitor information systems and protect information from unauthorized access or use, based on a periodic assessment of their information systems and the information that resides on the systems"	See User Security & Access. Our response to this topic, information protection requirement is the same as in item #10, above. [see item #10, above]
12	*II. Discussion, (A) Cybersecurity Risk Management Policies and Procedures (1) Required Elements of Advisers' and Funds' Policies and Procedures (c) Threat and Vulnerability Management*	This section in its entirety creates a requirement that leaves no room for specific situations where risks exist in a unique way. As such it over-prescribes how to identify and respond to threat. Instead, a better result will come from a risk assessment process. The risk assessment includes: • Assessment of risks in terms of likely frequency • Assessment of risks in terms of likely impact • Risk management with key controls to manage the risks • Risk management with mitigating controls that will act as fail-safe when key controls do not work.
13	*II. Discussion, (A) Cybersecurity Risk Management Policies and Procedures (1) Required Elements of Advisers' and Funds' Policies and Procedures (d) Cybersecurity Incident Response and Recovery*	See User Security & Access. Our response to this topic is the same as in item #10, above. [see item #10, above]

#	***Citation* followed by Proposed rule topic**	**Our Comment**
14	*II. Discussion, (A) Cybersecurity Risk Management Policies and Procedures (2) Annual Review and Required Written Reports*	This section in its entirety creates a requirement that is reasonable, **but it may not go far enough**: **more frequent reviews should be mandated than annually.** When it comes to cybersecurity of an organization with a large amount of confidential data and information, the more frequent review would likely be more effective than "annually". In addition, post-incident review should be performed, regardless of if the incident leads to a declared "breach". Incidents and breaches are not the same.
15	*II. Discussion, (A) Cybersecurity Risk Management Policies and Procedures (3) Fund Board Oversight*	**In our view, the Fund Board is where the reporting should go, and such reporting should go no farther, except as a confidential reporting to the FBI or other governmental agencies for the purpose of technical analysis.** The oversight should be done by the Fiduciary governance, and not by the public. The public, including investors, short-sellers, and cybercriminals should not be appraised of the roadmap of incidents. Instead, the floodgate should be protected by the fiduciary responsibility of the Board, and technical reporting – confidentially – to organizations such as NCIJTF or others who will maintain such details in confidence.
16	*II. Discussion, (A) Cybersecurity Risk Management Policies and Procedures (4) Recordkeeping*	We agree that a record keeping should be maintained at sufficient technical detail that would enable a through incident response and post-incident review, as well as sharing with professionals from law enforcement.

#	***Citation* followed by Proposed rule topic**	**Our Comment**
17	*II Discussion (B) Reporting of Significant Cybersecurity Incidents to the Commission* "We are proposing a new reporting rule requirement and related proposed Form ADV-C."	We agree that a reporting should be made, and we disagree that it should be public for the road map reasons we mentioned above [see items #5, #15, above].
18	*II. Discussion. (B) Reporting of Significant Cybersecurity Incidents to the Commission (1) Proposed Rule 204-6* "Proposed rule 204-6 would require investment advisers to report 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"	This rule is impractical. There should be a delineation between "incident" and "breach". Setting a timeline should not start with an incident which is a suspicion of a breach. Instead, such timeline should start once a breach is declared and fully assessed. A breach is the determination of unauthorized access have occurred. As stated now in the Proposed Rule, the timeline is nebulous. It should really start once the Fund Board receive a finalized breach or incident report.
19	*II. Discussion. (B) Reporting of Significant Cybersecurity Incidents to the Commission (2) Form ADV-C*	Form ADV-C is reasonable **if** it is maintained in confidence for the reasons identified herein [see items #5 and #15, above]
20	*II. Discussion (C) Disclosure of Cybersecurity Risks and Incidents* "We are also proposing amendments to certain forms used by advisers and funds to require the disclosure of cybersecurity risks and incidents to their investors and other market participants"	We oppose the public disclosure for the reasons above: in brief, it creates a roadmap of cybersecurity perimeter weak points for bad actors, as well as an opening for short sellers to manipulate the market [see items #5, #15, above].

#	***Citation* followed by Proposed rule topic**	**Our Comment**
21	*II. Discussion (C) Disclosure of Cybersecurity Risks and Incidents* *(3) Requirement to Deliver Certain Interim Brochure Amendments to Existing Clients (4) Proposed Amendments to Fund Registration Statements*	We oppose the public disclosure for the reasons above: in brief, it creates a roadmap of cybersecurity perimeter weak points for bad actors, as well as an opening for short sellers to manipulate the market [see items #5, #15, above].
22	*III. Economic Analysis*	In general, we agree that the cost/benefit of *performing* the tasks in the proposed rule are helpful for companies and equalize the "bad players" with the "good players", who are already doing all the right things. Some of the requirements, while reasonable as we stated above are likely already in place (for example, Risk Assessment). Advisers should be explicitly allowed to re-purpose risk assessments from other regulatory requirements for compliance with the Proposed Rule. Other requirements such as "access controls", or "multifactor authentication" are **over-prescriptive and are simply cumbersome** while imperative, so they do not add to the proposed regulation. The requirements that are technological in nature should not make it into the Proposed Rule. Instead, the **regulators should leave this to a Board monitored risk assessment to determine the technological responses to the assessed risks.**

#	***Citation* followed by Proposed rule topic**	**Our Comment**
23	*III. Economic Analysis*	While some of our responses herein imply a consideration of cost versus benefit, and efficiency versus effectiveness of various features of the Proposed Rule. Overall, our focus in this response is on the technological aspects of cybersecurity, and the risk assessment and risk management processes. Noted herein are only some of the responses we have about the "Economic Analysis" that accompanies the Proposed Rule.
24	*III. Economic Analysis (C) Baseline Cybersecurity Risks and Practices* "..best practice frameworks such as Carnegie Mellon University's Cyber Resilience Review, the NIST Framework, and similar offerings from cybersecurity consultants and product vendors are now frequently employed to assess and address institutional cybersecurity preparedness."	We recommend that the SEC consider utilizing a singular governmental standard such as NIST's cybersecurity risk standard. Any other *framework* – with are not a standard – such as Carnegie Mellon University's Cyber Resilience Review should be mapped to this singular standard. Applying a unified standards will create equalization among "bad plays" with their counter parts, the "good players". It will also eliminate an expectation gap and provide a clear guideline on how to proceed and comply. Absence of a standard could result in "false sense of comfort" for the SEC and the Advisers.

#	***Citation* followed by Proposed rule topic**	**Our Comment**
25	*III. Economic Analysis (C) Baseline Cybersecurity Risks and Practices (3) Market Structure* "A cybersecurity breach at an adviser that only offers advice on wealth allocation strategies may not have a significant negative effect on its clients: such adviser may not hold much client information beyond address, payment details, and the client's overall financial condition." and "Based on Form ADV filings up to October 31, 2021, there were 14,774 advisers with a total of $113 trillion in assets under management.155 Practically all (97%) of the advisers reported providing portfolio management services to their clients"	There appears to be an internal contradiction in this analysis. On the one hand, the ADV study shows that 97% of Advisers are at a low risk, on the other hand it appears that the Proposed Rule is established in order to increase the security over information held by the same low-risk Advisers. This is another reason why risk assessment, not prescribed controls within the Proposed Rule should be implemented. While Multifactor Authentication seems like a good idea for most Advisers, its is the specific makeup of each Adviser's risk portfolio that should govern their risks for a breach.
24	*IV. Paperwork Reduction Act Analysis* *K. Form N-3* "The proposed amendments to Form N-3 would require a description of any significant cybersecurity incident that has occurred in a fund's last two fiscal years."	Such disclosures could be disastrous for both the reporting Adviser as well as others with similar vulnerabilities, by publishing a road map of technological weakness. The road map that such a form will present could lead to additional exploitations of vulnerability. While a description to organizations such as NCIJTF or governmental agencies is appropriate, a public disclosure should **not** be made. [See items #5, #15, above]

###