PICKARD DJINIS AND PISARRI LLP
ATTORNEYS AT LAW
1990 M STREET, N.W., SUITE 660
WASHINGTON, D.C. 20036
WWW.PICKDJIN.COM

TELEPHONE
(202) 223-4418

FACSIMILE
(202) 331-3813

May 3, 2022

Filed Electronically

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

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

Dear Ms. Countryman:

Pickard Djinis and Pisarri LLP[1] is pleased to submit these comments in response to the above-referenced proposal that would impose extensive new cybersecurity compliance, disclosure, reporting and recordkeeping obligations on federally registered investment advisers and others.[2] Although it is beyond dispute that cybersecurity is critical to the safety and soundness of the capital markets and merits the Commission's attention, we regret that we cannot support all aspects of this proposal. We respectfully ask the Commission to revise the proposal before proceeding further with this important regulatory initiative.

Cybersecurity Risk Management Policies and Procedures

Proposed Advisers Act Rule 206(4)-9 would require federally regulated investment advisers to implement comprehensive cybersecurity risk management policies and procedures in order to "prevent fraudulent, deceptive, or manipulative acts, practices or courses of business within the meaning of section 206(4) of the Act." The proposed rule includes more than a dozen explicit requirements relating to risk assessment, user security and access, information protection, threat and vulnerability management and cybersecurity incident response and recovery, along with new annual review and documentation obligations. While purportedly designed to permit advisers to

[1] Pickard Djinis and Pisarri LLP is a law firm specializing in securities regulation relating to investment advisers, broker-dealers and service providers thereto. Our investment adviser client base ranges from federally registered firms with billions of dollars of assets under management to state-regulated solo practitioners. This letter reflects the views of a number of our federally regulated adviser clients.

[2] *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*; Release Nos. 33-11028, 34-94197, IA-5956, IC-34497; 87 Fed. Reg. 13524 (March 9, 2022), available at: https://www.sec.gov/rules/proposed/2022/33-11028.pdf ("Proposing Release"). These comments focus exclusively on the investment adviser components of the proposal, but parallel requirements are proposed for registered investment companies and business development companies.

tailor their cybersecurity policies and procedures to fit the nature and scope of their business, the highly prescriptive character of Rule 206(4)-9 would afford advisers little flexibility in practice.

We have four reservations about this rule.

1. The proposed rule would expose advisers to potential fraud liability for being the victims of other parties' misconduct.

Advisers Act Section 206(4) outlaws "fraudulent, deceptive, or manipulative" conduct by investment advisers. While cybercrime certainly involves fraud, deception and manipulation, an investment adviser who experiences a cybersecurity incident is a *victim* of such conduct, not its perpetrator. Unless the adviser makes a material misstatement or omission about its cyber risks or preparedness, or unless it recklessly disregards a known cyber threat or system weakness, it is hard to see how a failure to adopt the prescribed policies and procedures could rise to the level of fraud.

To illustrate this point, consider proposed Rule 206(4)-9(a)(3)(ii) which requires an adviser to contractually commit any service provider who receives, maintains or processes the adviser's confidential information to a range of specific cybersecurity practices. Should a service agreement fail to require one or more of the prescribed elements, the adviser could be deemed to have engaged in fraudulent, deceptive or manipulative conduct under the rule, even though no reasonable person would ever draw such a conclusion.

Exposing an adviser to the threat of a fraud determination for failure to comply with detailed procedural requirements—especially where the sufficiency of the adviser's procedures is likely to be evaluated in hindsight after a security breach—-will do little to protect investors but may have devastating consequences for the adviser.[3]

2. The proposed rule is inconsistent with principles-based regulation.

The Advisers Act establishes a principles-based regulatory regime grounded in the fiduciary duties of care and loyalty. This regime works best when advisers are given the leeway to structure their compliance efforts according to their particular circumstances. The Commission recognized this fact in 2003 when it adopted Rule 206(4)-7 (the "Compliance Program Rule"), saying, "[A]dvisers are too varied in their operations for the [rule] to impose a single set of universally applicable required elements."[4]

---

[3] For example, a finding that an adviser engaged in fraudulent conduct may preclude the adviser from competing for business from pension plans or other large institutional investors.

[4] *Compliance Programs of Investment Companies and Investment Advisers*, Advisers Act Rel. No. 2204 (Dec. 17, 2003), 68 Fed. Reg. 74714, 74715-16 (Dec. 24, 2003) ("Compliance Program Release"). In the (mercifully brief) adopting release accompanying this rule, the Commission identified the issues an adviser's compliance program should address "to the extent that they are relevant to that adviser." 68 Fed. Reg. at 74716.

But imposing a single set of universally applicable required elements is precisely what Rule 206(4)-9 would do. Although the Commission invites advisers to tailor the rule's many requirements to their own operations, as a practical matter, any deviation from an expansive application of each prescribed element would expose an adviser to the risk of adverse regulatory action.

The highly prescriptive nature of the proposed rule also entails a risk of obsolescence. Cybercriminals are notorious shape-shifters who are adept at staying one step ahead of victims' efforts to safeguard their systems and information. While the detailed elements of the proposed rule may reflect today's best practices, it is hard to predict what an effective cybersecurity compliance program will look like in the years to come. A less prescriptive rule would be more "evergreen" and thus, more effective in the long run.

3. The Commission has failed to demonstrate the need for a prescriptive new cybersecurity rule.

Investment advisers are already required to identify and manage their cybersecurity risks. This obligation derives in the first instance from advisers' overarching fiduciary duties, which require them to take steps to protect clients' interests from being placed at risk as a result of the advisers' inability to provide advisory services.[5] The Compliance Program Rule builds on this base, requiring advisers to implement policies and procedures, tailored to their particular circumstances, to prevent violations of their fiduciary and regulatory obligations.[6] Advisers are further required to test the sufficiency of these policies and procedures and the effectiveness of their implementation on at least an annual basis.

Along with these general requirements, investment advisers are subject to various specific requirements implicating cybersecurity. These include an obligation under Regulation S-P to "adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information."[7] And advisers subject to Regulation S-ID must implement written identity theft programs that include oversight of service providers.[8] Additional cybersecurity requirements are imposed on "qualified custodians" such as banks and broker-dealers who maintain physical custody of advisers' managed assets.[9]

Moreover, the SEC staff has issued extensive guidance identifying best practices to address a range of cybersecurity risks.[10] Unlike proposed Rule 206(4)-9, which would require every

[5] Proposing Release, 87 Fed. Reg. at 13526.

[6] Compliance Program Release at n. 22 and accompanying text.

[7] 17 CFR Part 248.30.

[8] 17 CFR Part 248.201-202.

[9] Proposing Release at text accompanying n. 133.

[10] *See, e.g.* SEC EXAMS Risk Alert, *Cybersecurity: Safeguarding Client Accounts against Credential Compromise* (Sep. 15, 2020), available at Risk Alert - Credential Compromise.pdf (sec.gov); SEC EXAMS Risk Alert, *Cybersecurity: Ransomware Alert* (Jul. 10, 2020), available at Risk Alert - Ransomware.pdf (sec.gov); SEC, EXAMS, *Cybersecurity and* Resiliency Observations (Jan. 27, 2020), available at OCIE

investment adviser to adopt the same cybersecurity program elements, the staff guidance acknowledges that the suitability of any suggested practice depends on the investment adviser's particular circumstances.

We do not believe the Commission has identified problems with the existing cybersecurity requirements sufficient to justify the imposition of an additional layer of prescriptive regulation. While expressing a sense that "some advisers" are not doing enough to identify and manage their cyber risks, the Commission offers no evidence of a widespread failure by advisory firms to address this mission-critical aspect of their businesses. On the contrary, the Commission acknowledges that cybersecurity best practice frameworks are "now frequently employed to assess and address institutional cybersecurity preparedness;" that the financial services industry is "one of the biggest spenders on cybersecurity measures;" and that firms undertake "increasingly costly efforts to prevent" cybercrime.[11] Nevertheless, relying on a survey of 27 mostly global financial companies, the Commission opines that financial services firms' "considerable" spending on cybersecurity "may nonetheless be inadequate."[12] Even so, the Commission admits that "the true extent of advisers' . . . underspending—and of failing to adopt industry-accepted cybersecurity 'best practices'—is impracticable to quantify."[13]

We respectfully submit that a vague sense—based on a survey of less than one percent of the industry—that investment advisers are not spending enough on cyber compliance is not a sufficient reason to adopt a prescriptive new anti-fraud rule under the Advisers Act.

4. The proposed rule would impose an undue burden on small advisers.

We appreciate the Commission's intent to craft a rule that is not overly burdensome or costly to implement, but fear that Rule 206(4)-9 falls short of that laudable goal. To the extent the proposed rule is designed to address perceived "underspending" on cyber compliance, the rule will impose a disproportionate burden on small advisers who have fewer resources to spend. While all advisers, regardless of size, need good cyber hygiene and should address the core areas covered by the proposed rule, all advisers do not need elaborate written policies and procedures for each granular element the rule identifies. To take one example, policies and procedures restricting access to adviser information systems on a "need to know" basis may be neither relevant nor practical for a firm with only a handful of employees. Given the fact that roughly one-third of federally registered

---

Cybersecurity and Resiliency Observations.pdf; EXAMS Risk Alert, Cybersecurity: Ransomware Alert (May 17, 2017), available at: Cybersecurity: Ransomware Alert; and SEC Division of Investment Management Guidance Update, *Cybersecurity Guidance* (Apr. 2015), available at IM Guidance Update: Cybersecurity Guidance.

[11] Proposing Release, 87 Fed. Reg. at 13545.

[12] *Id.*, *citing* Institute of International Finance, *IIF/McKinsey Cyber Resilience Survey* (Mar. 2020), available at cyber_resilience_survey_3.20.2020_print.pdf (iif.com).

[13] Proposing Release, 87 Fed. Reg. at 13545.

investment advisers have five or fewer employees, and more than half have ten or fewer employees, this is a significant problem indeed.[14]

Some mandatory elements are not just impractical, but may actually be impossible for small firms. For example, requiring advisers to contractually commit their service providers to implement and maintain measures tracking the elements of the rule assumes that small advisers have a bargaining power that simply does not exist. Service providers' contracts are typically non-negotiable, and their willingness to have their practices monitored by every small adviser they deal with is limited, at best. Requirements such as those proposed in 206(4)-9(a)(3)(ii) are tripwires for a large segment of the investment adviser industry.

There are better ways to foster good cyber hygiene among investment advisers.

In light of the foregoing, we urge the Commission to consider a different path to investment adviser cybersecurity. One possible approach would be for the Commission to issue a comprehensive interpretive release synthesizing the existing regulatory requirements and staff guidance on the topic. This could serve as the foundation for periodic updates from SEC staff informing the industry about new cyber risks and best practices, incorporating both information from examinations and aggregate data from the incident reports contemplated by proposed Rule 204-6.

If the Commission continues to see a need for new rulemaking, we ask that the new rule not be adopted under the Advisers Act's anti-fraud provision, but under some other authority, such as Section 203(e)(6), 204 or 211. We further ask that any such rule be principles-based and not overly prescriptive. Finally, we ask the Commission to synthesize any new rule with existing regulations, which may require amendments to Reg S-P and Reg S-ID to eliminate duplication.

If Commission decides to pursue Rule 206(4)-9, we ask that exemptions be added as appropriate, for advisers with fewer than 50 employees.[15] At the very least, the Commission should not make the proposal worse by mandating additional costly elements such as audits by independent third parties, obligations to assess the compliance of service providers with their

---

[14] See IAA-NRS *Investment Adviser Industry Snapshot* 2021 (July 2021), available at Investment_Adviser_Industry_Snapshot_2021.pdf (investmentadviser.org) at 41.

[15] We believe such firms are appropriately characterized as small advisers. On a related note, we submit that the standard the Commission employs to identify "small entities" for purposes of the Regulatory Flexibility Act is flawed because the obsolete assets-under-management test incorporated into Advisers Act Rule 0-7(a) ensures that the Commission's assessment of the effect of its rules on small advisers will eliminate virtually the entire population of federal registrants from consideration. Applying this standard in the instant rulemaking, for example, results in only 579 of 14,774 registered advisers being designated as small entities. Proposing Release, 87 Fed. Reg. at 13578. Ironically, at least some of those 579 firms are large, well-resourced data providers whose activities qualify them for federal registration notwithstanding the fact that they do not manage assets.

Because an adviser's ability to shoulder regulatory compliance burdens depends on its human and financial resources, we believe that Rule 0-7 should be amended to identify small entities by looking at their staff and revenues, not their AUM.

contractual cybersecurity obligations, or minimum qualifications for personnel responsible for implementing advisers' cybersecurity programs.

Reporting

In order to play an effective role in safeguarding the capital markets from cybercrime, the Commission needs timely and accurate information about significant cybersecurity incidents. For this reason we support the adoption of proposed Rule 204-6 and proposed Form ADV-C, with certain modifications. For example, we have concerns about requiring an initial report within 48 hours after the adviser has a reasonable basis to conclude that an incident has occurred or is occurring. First, we observe that what "reasonable" looks like in hindsight may be very different from how it appears in real time; we would hope that this requirement does not become an excuse to second-guess advisers who act in good faith under difficult circumstances. More importantly, we fear that such a short deadline will divert the adviser's attention from the critical task of addressing the breach. We ask that advisers be given 72 hours or longer to file an initial incident report.

We also have concerns about requiring an adviser to amend its report within 48 hours after previously reported information becomes materially inaccurate or new material information about an incident is discovered. For one thing there may be a lag between when information "becomes materially inaccurate" and when the adviser learns that it is so. Moreover, in the aftermath of a cyberattack, material new information may constantly unfold, in which case, the adviser's focus should be on addressing that information, not filing successive regulatory reports.[16] Although we agree that a Form ADV-C amendment should be filed after a significant cybersecurity incident is resolved or an internal investigation regarding a previously disclosed incident is closed, we do not think interim amendments are a wise idea.

As for the cybersecurity incident report itself, we agree that a structured format would allow the Commission and its staff to assess cybersecurity incident trends across the industry and address threats on a systemic basis. We believe, however, that some items in proposed Form ADV-C are too granular,[17] while others are irrelevant.[18] In any event, we firmly believe that these reports must be kept confidential. Public disclosure of the information reported on Form ADV-C could hinder an adviser's ability to mitigate or remediate a cybersecurity incident and could divulge vulnerabilities that could be exploited in future attacks. Finally, we support the use of the IARD for filing incident reports, but urge the Commission to provide safe alternatives, such as secure email and a paper filing option in case the reported incident has compromised the adviser's access to the internet.[19]

---

[16] This is particularly so if, as the SEC predicts, the adviser could engage in a "productive dialogue" with Commission staff after an initial incident report, during which the adviser can provide the staff "with any additional information as necessary." Proposing Release, 87 Fed. Reg. at 13537.

[17] *See, e.g.,* Items 11 and 12.

[18] *See, e.g.,* Item 16.

[19] An adviser should not have to file an application for a hardship exemption on Form ADV-H in order to avail itself of a paper filing option. A certification of the adviser's inability to file Form ADV-C through the IARD should be added to the incident report itself.

Disclosure

In designing any cybersecurity risk and incident disclosure requirement two considerations are paramount. First, the disclosure must convey meaningful information to its intended audience, and second, the disclosure must not reveal information that could be used by threat actors to launch future attacks. Although we do not object in theory to the addition of cybersecurity disclosure to Form ADV Part 2A, we are not convinced that Item 20, as proposed, adequately addresses either of these considerations.

With regard to the first element, Item 20 would oblige advisers to describe the cybersecurity risks that could materially affect the advisory services they offer, which seems benign enough. However, the additional requirement to describe how the adviser "assesses, prioritizes, and addresses those risks" could be problematic. Simply disclosing that the adviser periodically assesses its risks and categorizes and prioritizes those risks based on an inventory of the components of its information systems and the information residing therein may be of little value to clients and potential clients. However, revealing the adviser's actual assessment of the severity of any particular risk relative to other risks and the steps taken to address that risk may create its own set of risks. Public disclosure of this type of information may give potential perpetrators a detailed view of the firm's vulnerabilities and capacity to mitigate breaches.

The second prong of Item 20 would oblige an adviser to describe any cybersecurity incident that occurred within the last two fiscal years that has significantly disrupted the adviser's operations or has led to the unauthorized access or use of adviser information resulting in substantial harm to the adviser or its clients. This disclosure must include information about the details of the breach and whether the incident or its remediation is ongoing. For the reasons discussed above, public disclosure of the details of an ongoing cyberattack and a firm's response thereto would do more harm than good; any information being held in confidence on Form ADV-C does not belong in Form ADV Part 2A.

As to both prongs of proposed Item 20, it appears that the Commission lacks sufficient information about the value investors place on advisers' cybersecurity practices and their ability to distinguish between incidents caused by chance and those resulting from inadequate cyber risk management.[20] For this reason, we respectfully suggest that the Commission convene a focus group to assess client preferences and comprehension and explore alternate ways to inform clients directly if the security of their personal information has been compromised.

* * * * *

[20] Proposing Release, 87 Fed. Reg. at 13552 and 13553. Because, to some extent, cyber incidents are a matter of chance, we believe that disclosing the *absence* of a cybersecurity incident in the past two fiscal years could be misleading.

We appreciate the opportunity to submit these comments. We would be happy to supply any additional information you may desire about the matters discussed above. Kindly contact the undersigned at 202.223.4418 for further assistance.

Respectfully submitted,

Mari-Anne Pisarri

cc: The Honorable Gary Gensler, Chairman
The Honorable Hester M. Peirce
The Honorable Allison H. Lee
The Honorable Caroline A. Crenshaw
William A. Birdthistle, Director, Division of Investment Management