sifma
Invested in America

sifma
asset management group

April 11, 2022

Submitted electronically via SEC.gov
Vanessa Countryman, Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

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

Dear Secretary Countryman:

The Securities Industry and Financial Markets Association ("SIFMA")[1] and SIFMA Asset Management Group ("SIFMA AMG") appreciate the opportunity to comment on the proposed new cybersecurity risk management rules and amendments issued by the Securities and Exchange Commission ("Commission" or "SEC"). On February 9, 2022, the Commission published a Release for Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies containing proposals that, if adopted, would establish a new cybersecurity incident reporting and disclosure regime and require registered investment advisers ("advisers") and investment companies ("funds") to implement policies and procedures designed to address cyber risks.[2] We appreciate the opportunity to address various issues despite the short comment period for this extensive set of proposed rules and amendments.[3]

[1] SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our members, we advocate for legislation, regulation, and business policy affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

[2] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Release Nos. 33-11028, IA-5956, IC-34497, 87 Fed. Reg. 13524 (proposed Feb. 9, 2022) (to be codified at 17 C.F.R. pts. 230, 232, 239, 270, 274, 275, 279).

[3] Given the complexity of these proposed rules, the short comment period is not adequate to address all reporting, disclosure, and cyber policy and procedure proposals. *See* Joint Comment Letter from SIFMA and other associations to the Commission on the "Importance of Appropriate Length of Comment Periods" (April 5, 2022), *available at* https://www.sifma.org/resources/submissions/importance-of-appropriate-length-of-comment-periods ("The number of rule proposals, the complexity of the issues being tackled, the potential interconnectedness of the proposals, and lurking possible negative, unintended consequences should be considered when setting a proposal's comment period. The Associations are concerned that the Commission's current approach to comment period lengths does not take such an approach and ultimately does not comport with the spirit of the APA and applicable federal guidelines on rulemaking procedure.").

1. Executive Summary

SIFMA believes the Commission should reconsider its proposals in light of the following:

- The Commission's proposal of adviser requirements under the antifraud provision of the Investment Advisers Act of 1940 ("Advisers Act") goes beyond that statutory authority. The Commission should instead provide guidance to advisers and funds and coordinate with other federal financial regulators and the Cybersecurity and Infrastructure Security Agency ("CISA") under recently adopted critical infrastructure reporting legislation.

- If the Commission is committed to creating an additional reporting regime, its proposed 48-hour reporting protocol, involving the onerous completion and submission of Form ADV-C, is unworkable and will not yield useful information for the Commission. The Commission should instead adopt a bifurcated approach: an informal short form notification followed by a more detailed report, without sensitive data, to be submitted after the adviser has had sufficient time to investigate a cyber intrusion.

- An abbreviated initial notification would align with other regulatory reporting requirements; such harmonization would in turn reduce unnecessary compliance burdens, maximizing an institution's ability to focus on protecting clients and investors during a cyber crisis. Duplicating reporting requirements is not only inefficient but can damage coordinated cyber incident response at the enterprise level.

- The Commission should provide assurance and documentation of how confidential and high-risk information submitted to the Commission will be protected from intrusion.

- Public disclosure of detailed information relating to cybersecurity incidents or risks is unnecessary and may put members or the financial system at risk.

- The proposed disclosure requirements, particularly the suggested vehicles for disclosure (amended Form ADV Part 2A and the fund prospectus) are onerous, and delivery would require significant burdens and costs. It is too burdensome to require that advisers continually update or revise disclosures and that funds disclose cybersecurity incidents *currently affecting it* and file prospectus supplements.

- The Commission should adopt a principles-based approach to risk management, as opposed to a "one-size-fits-all" system of policy and control prescriptions.

- To the extent a final rule does include cyber-program requirements or best-practice recommendations, institutions must be able to implement those measures in accordance with an internal assessment; otherwise, the requirements will be too prescriptive.

- Boards should exercise some oversight of cybersecurity programs but should not be compelled to formally approve or review all cyber policies and functions.

2. Commission Overreach and Use of Antifraud Provision

We share the Commission's goal of protecting investors, market participants, and the financial services industry from cyber-attacks. However, as a threshold matter, we are concerned that the Commission has chosen to rely on its antifraud authority in Section 206 of the Advisers Act, which prohibits an adviser from engaging in "any act, practice, or course of business which is fraudulent, deceptive, or manipulative."[4] This antifraud provision is not an appropriate source of statutory authority for cyber hygiene rules and could lead to unwarranted Commission enforcement action.

Institutions today are already working to strengthen their cyber defenses to help avoid being victimized by threat actors. The Commission should focus on assisting institutions in these efforts, perhaps by issuing guidance on cyber hygiene that addresses program expectations. In contrast, under proposed rule 206(4)-9, it would be unlawful for an adviser to provide any investment advice to clients without first adopting certain prescriptive cybersecurity policies and procedures.[5] We cannot help but question whether the Advisers Act will support the weight that the Commission is trying to place on it.

We imagine the Commission intends to use the Advisers Act's antifraud provision to encourage institutions to prioritize cybersecurity, but we are concerned about the appropriateness and ultimate effectiveness of this approach, particularly when institutions today are already working to strengthen their cyber defenses to help avoid being victimized by threat actors.

In our view, the Commission should assist institutions enhance cybersecurity programs instead of drafting new rules that punish advisers if there is a perceived deficiency in security measures.

Our concern about the Commission's overreach is not limited to the use of the Advisers Act. We also question whether it is appropriate for the Commission to propose and possibly finalize additional cyber reporting obligations at a moment when both the executive and legislative branches of the federal government are working toward centralizing and streamlining the fragmented incident reporting regime. In fact, as we draft this letter, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which was unanimously passed by the Senate and will require critical infrastructure institutions to report significant cyber incidents and all ransom payments to the Department of Homeland Security's CISA.[6] The Act gives CISA the authority to define which entities will be subject to the Act's reporting obligations, and CISA will use its rulemaking power to regulate entities that operate

[4] 15 U.S.C. 80b-6(4).

[5] *See* 87 Fed. Reg. 13592 ("As a means reasonably designed to prevent fraudulent, deceptive, or manipulative acts, practices, or courses of business within the meaning of section 206(4) of the Act (15 U.S.C. 80b6(4)), it is unlawful for any investment adviser registered or required to be registered under section 203 of the Investment Advisers Act of 1940 (15 U.S.C. 80b–3) to provide investment advice to clients unless the adviser adopts and implements written policies and procedures that are reasonably designed to address the adviser's cybersecurity risks…").

[6] Consolidated Appropriations Act, 2022, Division Y, Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), H.R. 2471, 117th Cong. (2021-2022). Covered entities must report cyber incidents within 72 hours and ransomware payments within 24 hours. Separately, the President has designated the Departments of Homeland Security and Justice as key components of the national cybersecurity system. *See* Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021) (The Secretary of Homeland Security, in consultation with the Attorney General, should establish the Cyber Safety Review Board that comprises of representatives of the Department of Justice and other departments).

the nation's critical infrastructure.[7] At a minimum, CISA will likely define "covered entities" to encompass the 16 sectors currently considered "critical infrastructure" under Presidential Policy Directive 21, which includes financial services. Notably, the Act provides a mechanism for CISA to disseminate anonymized information to other government agencies and includes some liability and freedom-of-information request protections for reports describing covered cybersecurity incidents.[8]

With this development in mind, we encourage the Commission, a regulatory enforcement agency, to respect the intent of Congress and accordingly pursue the recently invigorated effort to establish a more judicious standardized federal method for reporting cybersecurity incidents, with CISA responsible for receiving and distributing information to relevant stakeholders.[9] A single federal notification regime would solve the serious reporting-related compliance burdens detailed herein.

Government agencies must collaborate to protect critical infrastructure and build sound cybersecurity frameworks while considering important private sector concerns about securing risk information and establishing efficient exchanges of information that avoid overburdening compliant institutions. In that spirit, the Commission should not adopt a role that causes financial services companies subject to potential CISA requirements to report the same information to the Commission during the middle of a cybersecurity event.

While we support the policy goals behind the proposed reporting, disclosure, and cyber hygiene requirements, we have concerns about the Commission's use of Advisers Act authority, about its deviation from current Congressional efforts to centralize cyber-related communication channels, and about the unnecessary additional burdens that the proposed rules would impose on advisers and funds.

We respectfully implore the Commission to reconsider finalizing its proposed cybersecurity regulations and particularly refrain from promulgating cyber rules until CIRCIA and related regulations from CISA come into effect. Should the Commission nonetheless proceed, we believe that significant revision is warranted in several areas.

3. Confidential Incident Reporting to the Commission

a. Overview of Proposed Rule 204-6 under the Advisers Act

Proposed rule 204-6 would require advisers to report to the Commission on a confidential basis "significant adviser cybersecurity incidents" and "significant fund cybersecurity incidents." The Commission defines a notification-triggering "significant adviser cybersecurity incident" as a "cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: (1) Substantial harm to the adviser, or

[7] CIRCIA, § 2240(5).
[8] *Id.* at § 2245(b).
[9] We recognize the difference between notification for cybersecurity purposes and notification for enforcement purposes and believe that, with respect to the Commission, the latter can be handled through a subsequent report.

(2) substantial harm to a client, or an investor in a private fund, whose information was accessed."[10] The Commission defines "cybersecurity incident" as an "unauthorized occurrence on or conducted through [an adviser's or a registered fund's] information systems that jeopardizes the confidentiality, integrity, or availability of [an adviser's or a registered fund's] information systems or any [adviser or registered fund] information residing therein."[11]

Under the proposed rule, advisers would notify the Commission of significant adviser/fund cybersecurity incidents through a new electronic Form ADV-C on the Investment Adviser Registration Depository (IARD) no more than 48 hours after having a "reasonable basis to conclude that any such incident has occurred or is occurring."[12] Additionally, rule 204-6 would require each adviser to amend any previously filed Form ADV-C no more than 48 hours after: (1) information previously reported becomes "materially inaccurate"; (2) new material information is discovered; or (3) any internal investigation pertaining to an incident is closed, or the incident is resolved.[13]

b. **Discussion of Comments on Proposed Rule 204-6 under the Advisers Act**

i. **The proposed 48-hour reporting regime will not yield useful information for the Commission because there is not sufficient time to investigate and provide a detailed report.**

The Commission observes that its proposed reporting requirement would better enable it to "monitor and evaluate the effects of [a] cybersecurity incident on an adviser and its clients or a fund and its investors" and "assess the potential systemic risks affecting financial markets more broadly."[14] Our members will benefit from careful monitoring of cyber-related occurrences that may, in certain instances, signal a widespread security issue requiring the immediate attention of financial institutions, as well as other federal and state agencies. To that end, we recognize the importance of effective incident reporting, and proper information sharing, for detecting and addressing cyber threats, and we note that many of our members currently communicate cybersecurity issues with a range of regulators on both a voluntary and obligatory basis.

While our members support the Commission's goal of maintaining awareness of emergent cyber issues and protecting investors, the proposed reporting requirement, which involves drafting responses to proposed Form ADV-C questions in an unreasonably short time, is not an effective way to achieve that objective.

The abbreviated 48-hour reporting timeframe will not yield the disclosure the Commission seeks. If the Commission is committed to implementing a new reporting regime, it should accordingly adopt a bifurcated notification/reporting framework with a short confidential initial notification within 48 hours (to alert the Commission that there may be a significant

[10] 87 Fed. Reg. 13536. The Commission observes in a footnote that this proposed definition is "substantially similar to the proposed definition of 'significant fund cybersecurity incident' for funds." *Id.* at n.60.
[11] *Id.* at 13529 n.27.
[12] *Id.* at 13592.
[13] *Id.* at 13577.
[14] *See id.* at 13536 ("For example, these reports could assist the Commission in identifying patterns and trends across registrants, including widespread cybersecurity incidents affecting multiple advisers and funds.").

cybersecurity incident), followed by a confidential report (to ensure the Commission is able to receive valuable risk information and monitor cyber events).[15]

Our dual notification/reporting proposal strikes a balance between promptly notifying the Commission of essential information during an emergent cyber issue and avoiding burdening firms with longer reports during critical incident response periods. It would also align with other reporting regimes, including the recently-adopted Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers ("Banking Rule"), which requires covered financial institutions to simply notify a primary federal regulator of certain computer-security incidents through any form of written or oral communication.[16]

ii. **The proposed reporting requirement on Form ADV-C within 48 hours is unduly burdensome, duplicative, and may result in inaccurate reporting.**

We observe that the Commission commendably attempted to avoid conflicts with other federal rules when it drafted and proposed rule 204-6.[17] However, reporting different aspects of the same incident at different times to different regulators is not only burdensome but may ultimately create misunderstandings, confusion, and inconsistencies that can become problematic. Even if reporting requirements do not directly conflict, the request for similar but different information about a particular intrusion injects confusion into the incident response and compliance process. If the Commission is indeed committed to enacting a separate reporting regime, we implore it to revise the requirement by harmonizing it with other regulations, particularly with the Banking Rule and future CISA requirements under CIRCIA.

The current reporting requirement adds an onerous layer to the existing complex cyber reporting regime. Many of our members already report certain cybersecurity incidents to a range of other federal regulators, including:

- the Federal Deposit Insurance Corporation ("FDIC"),
- the Office of the Comptroller of Currency ("OCC"),
- the Federal Reserve System ("Federal Reserve"),
- U.S. state agencies, such as the New York State Department of Financial Services ("NYDFS"),
- Foreign regulators in jurisdictions where the member does business, and

[15] We emphasize the difference between an abbreviated *notification*, meant to provide the Commission with an alert regarding cybersecurity risks and a more extensive *report* with the type of information the Commission seeks from Form ADV-C.

[16] *See* 86 Fed. Reg. 66424 (to be codified at 12 C.F.R. pts. 53, 225, 304) (compliance date May 1, 2022).

[17] *See* 87 Fed. Reg. 13581 ("There are no duplicative, overlapping, or conflicting Federal rules with respect to proposed rule 204-6.").

- CISA (Congress recently created further requirements for reporting by critical infrastructure, as noted above).[18]

Over the past few years, regulators around the globe have proposed or finalized more than 30 new cybersecurity related rules impacting the financial services industry.[19] There are currently at least 11 U.S. federal agencies that impose some cybersecurity requirement on financial services institutions—including various reporting requirements—in addition to state obligations and self-regulatory standards from organizations like the Financial Industry Regulatory Authority ("FINRA") and the National Futures Association ("NFA").[20] The current cyber incident reporting landscape is thus characterized by fragmentation with differing time, materiality, and information requirements among various regulators. These numerous requirements increase costs for firms, which must divert resources from mitigating cyber issues to preparing to meet regulatory obligations. In fact, some large firms report that approximately 40 percent of corporate cybersecurity activities are focused on regulatory reporting rather than security.[21]

Filing Form ADV-C does not appear to be a simple additional task, especially in the middle of incident response, when focus should be directed toward preventing or mitigating harm to clients or investors and not filing, amending, and refiling forms. While the Commission generally structured Form ADV-C as a series of check-the-box and fill-in-the-blank questions, the form nevertheless requires 16 separate items, including information about the adviser, background information about the incident, substantive information about the nature and scope of the incident (i.e. any effect on "critical operations"; actions taken or planned actions to recover from the incident; whether data was stolen, altered, accessed or used for an unauthorized purpose; whether the incident has been disclosed to clients or investors),[22] and cybersecurity insurance information.[23] All responses to questions in ADV-C, particularly the fill-in-the-blank free-text responses, would take time to analyze, draft, and then circulate to stakeholders, including risk and legal functions (and possibly outside counsel), operations functions, COOs, firm administration employees, and so on. Moreover, different advisers may involve different legal coverage as well as different CCOs, who would need to sign off on filings.[24]

The information the Commission seeks from Form ADV-C, particularly about the nature and scope of a cybersecurity incident, is not always discernible within 48 hours of a cyber-attack, when an

---

[18] *See* CIRCIA, *supra* note 6.

[19] Data Security: Vulnerabilities and Opportunities for Improvement: Hearing Before the H. Subcomm. on the Financial Institutions and Consumer Credit, 115th Cong., 8 (2017) (written testimony of Kenneth E. Bentsen, Jr., President and CEO, SIFMA), *available at* https://www.congress.gov/115/meeting/house/106582/witnesses/HHRG-115-BA15-Wstate-BentsenK-20171101.pdf.

[20] *Id.*

[21] *Id.*

[22] We note that "critical operations" should not be defined. *See* 87 Fed. Reg. 13536 n.60 ("We view critical operations as including investment, trading, reporting, and risk management of an adviser or fund as well as operating in accordance with the Federal securities laws."). What is considered "critical" will vary across organizations, so this term should allow for that flexibility. Similarly, no quantitative amount should be established because it would result in arbitrary decisions. There is no simple way to establish whether a firm is operating at 75 percent or 80 percent of operations (compared with measuring output of a firm that manufactures physical products).

[23] 87 Fed. Reg. 13538-39.

[24] It is also worth noting that the legal or compliance personnel managing filings would not actually be the source of the information reported in the notice. To that end, firms would need to develop new processes to inform impacted ADV coverage for advisers/funds of a significant cybersecurity incident and relevant responses in the ADV-C.

institution may still be attempting to understand the edges of an intrusion, especially whether there is reasonable basis to conclude the adviser or its clients have suffered any harm. As noted above, institutions, particularly registered funds, need time to ensure that proper functions—appropriate technology and compliance personnel, outside counsel, and board members in some cases—can review an ADV-C filing or amended filing. The proposed 48-hour window does not appear to provide enough time to properly disclose and review information for all 16 items; even if it does in some cases, the abbreviated reporting window will likely lead to an imbalanced distribution of resources, with more time and energy devoted to regulatory reporting and related administrative tasks than to incident response and recovery.

The proposed reporting rule would unnecessarily burden financial institutions at critical crisis response times and ultimately siphon resources that should be directed toward managing an incident and protecting clients and investors.

Institutions need time to investigate and understand cyber intrusions before determining the nature and scope of the incident or whether an incident is even a reportable event. The import of complex cybersecurity incidents may not be apparent for weeks or even months. The National Security Agency ("NSA") notes that the average time to identify an adversarial presence within an enterprise network is 191 days, which is more than sufficient time to "wreak havoc" on a system.[25] While some cyber events may be patent, such as a network being taken down by ransomware, the implications of a particular incident can involve weeks of analysis. For instance, the Department of Justice ("DOJ") was reportedly subject to the SolarWinds intrusion long before the malware was identified; indeed, the DOJ apparently spotted rogue traffic, but initially reached the inaccurate conclusion that it had not been subject to any attack.[26] If the Commission requires reporting within 48 hours, it may inadvertently encourage the sort of cursory analysis undertaken by the DOJ in the rush to reach a conclusion as to whether a reportable incident exists.[27]

Additionally, the Commission's ongoing reporting requirement would multiply the burden institutions face. Given the evolving nature of incident investigation and response, the proposed rule's requirement that Form ADV-C amendments must be completed within an unreasonably short 48-hour window would likely entail frequent formal updates and over reporting that would

[25] NATIONAL SECURITY AGENCY, CYBERSECURITY INFORMATION: CONTINUOUSLY HUNT FOR NETWORK INTRUSIONS 1 (2019), *available at* https://media.defense.gov/2019/Sep/09/2002180360/-1/1/0/Continuously%20Hunt%20for%20Network%20Intrusions%20-%20Copy.pdf.

[26] *See* Zoe Strozewski, *Kremlin-Backed Hackers Still Stealing U.S. Data 'Relevant to Russian Interests': Report*, NEWSWEEK (Dec. 6, 2021, 12:47 PM), https://www.newsweek.com/kremlin-backed-hackers-still-stealing-us-data-relevant-russian-interests-report-1656462 ("The SolarWinds hack exploited vulnerabilities in the software supply-chain system and went undetected for most of 2020 despite compromises at a broad swath of federal agencies—including the Justice Department—and dozens of companies, primarily telecommunications and information technology providers and including Mandiant and Microsoft.").

[27] The Commission asks whether it should require that advisers and funds respond to cybersecurity incidents within a specific timeframe, and we do not think this is advisable. *See* 87 Fed. Reg. 13533 (Comment Request #16). In many cases, threat actors have been found to have been inside networks for months before discovery. Upon discovery of a cybersecurity incident, firms react quickly because it is often in their best interest to do so from an operational, legal, and reputational standpoint. The response and response time will vary based on the particular firm and its capabilities. For example, large firms often triage and prioritize incidents based on severity, which impacts response times. Imposing a specific response time could force companies to respond to less significant incidents to meet legal requirements at the expense of dedicating resources to incidents that should take priority.

not be useful to the Commission.[28] Though some organizations have dedicated ADV teams, those teams manage other regulatory developments, special projects, policies and procedures, and training, while also being involved in overseeing regulatory filings and exams. In short, even large organizations with greater resources would find it difficult to comply with the proposed ongoing reporting requirement. Under our proposal, an adviser would presumably remain in informal contact with the Commission after submitting its initial notice and would submit a singular report at the conclusion of the adviser's factual investigation.

Not all intrusions are inherently cause for an immediate regulatory report that seeks background information and substantive analysis. Some intrusions are indeed subtle but destructive, while others attempt to make a spectacle, such as defacing a website, but involve no real harm. Thoughtful forensic analysis requires some time, and we implore the Commission to avoid creating a process of rushed, abbreviated incident analysis.

iii. **Incidents involving third-party service providers require additional time for investigation and reporting.**

The Commission's proposed 48-hour reporting deadline does not seem to account for the fact that an intrusion may involve a third-party service provider—an additional entanglement that may require more time for investigation. We are particularly concerned about the feasibility of firms reporting incidents occurring outside of their control or technology estate within the short 48-hour deadline.[29] In many cases, a third-party service provider could be responding to inquiries from hundreds, or even thousands, of clients apart from the regulated entity, all while working to secure and remediate its own information systems.

To that end, we propose that the Commission specify that the clock start running only after an adviser or fund has determined that a significant cybersecurity incident has occurred, regardless of any determination or notification made by a service provider.

iv. **The Commission should coordinate with other federal cybersecurity resources and work toward regulatory harmonization.**

While we agree that the Commission should be well-positioned to monitor emerging cyber threats in order to protect investors, institutions, and the financial services industry, we do not believe the most effective way to do so is to exclusively add more regulation to the already voluminous cyber reporting regime. Rather, regulators like the Commission could enhance cybersecurity by plugging into a unified and streamlined reporting framework and engaging in appropriate information sharing.

As detailed above, the Commission should ensure that its efforts proceed in full coordination with CISA and other agencies and organizations gathering cybersecurity information, while

[28] One member reports that when a material amendment to Form ADV-C requires an other-than-annual update, the firm files the amendment within 30 days, and significant time and resources are involved in coordinating that single amendment.

[29] Relatedly, we request the Commission ensure that advisers/funds will not face enforcement sanctions should a service provider fail to disclose cyber incident information or be in violation of any requirements of the proposed rules.

recognizing that hackers do not respect the distinctions in jurisdiction of various prudential regulators or sectoral boundaries. The same ransomware gang could easily impact hospitals, banks, investment advisers, and pipelines.

We are encouraged by the Commission's expressed commitment to coordination. Recently, for example, Chair Gensler referenced comments made by the Director of CISA, Jen Easterly, who noted that "cybersecurity is a team sport" and "each and every one of us are a member of Team Cyber."[30] Chair Gensler observed that CISA and the Federal Bureau of Investigation ("FBI") "captain Team Cyber" and that the Commission "has a role to play as well."[31] We agree with Chair Gensler's assessment and accordingly encourage the Commission to rally around the idea of a centralized cybersecurity reporting regime. Coordination with other regulators on threat information sharing and propagation of evolving best practices will enable the Commission to protect investors more effectively.

v. Recommendation: A 2-Part Notification and Reporting Regime

If the Commission adopts a new incident reporting framework, it is imperative that the scope of the requirement is tailored, and the method of reporting is flexible and efficient. Regulators need both *timely* and *accurate* information, but these are two different, sometimes conflicting, goals. The current proposal, which requires the nearly impossible task of drafting, approving, and filing Form ADV-C within an exceptionally narrow window, could lead to errors and inaccuracies in the information reported to the Commission.

We propose the Commission adopt a bifurcated notification/reporting regime. Under this system, advisers would provide an initial, abbreviated notification that a significant cyber incident was determined to have occurred followed by a more detailed report—a tailored version of Form ADV-C, omitting certain sensitive data, such as remediation, disclosure, and cyber-insurance information, because this information is not necessary for the Commission to carry out its articulated monitoring objectives. In particular, an adviser's cyber insurance policy (or lack thereof) is not indicative of the potential effect a significant cybersecurity incident could have on an adviser's clients, the adviser's response to the incident, its cyber hygiene, or its ability to cover costs associated with the incident. This information should not be required as it is not relevant to the Commission's goal of "understanding the potential effect [a significant cybersecurity incident] could have on an adviser's clients."[32] We also hesitate to provide the Commission with sensitive data—particularly risk information—without having a clear sense of the security measures and controls the Commission intends to implement for its repository of reporting information.

An early, short-form notification within 48 hours would ensure the Commission receives timely notice of an emergent cyber issue while allowing firms to take appropriate steps to understand and mitigate that issue. A subsequent report would provide the Commission with analysis of a

[30] Gary Gensler, Chairman, SEC, Address at Northwestern Pritzker School of Law's Annual Securities Regulation Institute (Jan. 24, 2022), *available at* https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124.
[31] *Id.*
[32] 87 Fed. Reg. 13539.

significant cybersecurity incident, while minimizing the chance that inaccurate information will be disclosed and disseminated to other institutions or regulators.[33]

We also recommend that the Commission trigger notice upon the "determination" of significant cybersecurity incident, as opposed to requiring advisers or funds to provide notice based on their having a "reasonable basis to conclude that any such incident has occurred or is occurring."[34] A more targeted "determination" threshold would align with other standards and ensure that advisers have a clear sense of when to notify the Commission following the detection of a cyber intrusion.

Our members strongly believe that a bifurcated notification/reporting system, triggered upon the determination of a significant cybersecurity incident, would achieve the Commission's goals of information-collection to maintain awareness of emerging industry-wide cyber risks without overwhelming institutions or adding confusion to the reporting process.

(1) **An abbreviated initial notification would harmonize with other regulatory standards and reduce compliance burdens.**

Our proposed initial limited notification would align with other regulatory obligations and we again emphasize the importance of consistency in this area. Under the Banking Rule,[35] for example, a covered entity is required to provide only a "simple notice" to its primary federal regulator about a notification incident.[36] The Banking Rule's reporting obligation does not require any assessment, analysis, or specific information other than that a notification incident has occurred.[37] Moreover, the rule does not prescribe a specified form or template for delivery: notice can be provided by telephone or email.[38] We believe that this flexible format, and specifically the option to deliver notice by phone, will not only encourage candor in reporting, but will also ensure that a line of communication to the Commission remains open in the event a ransomware or denial-of-service (DoS) attack cuts off a firm's internet pipeline. During a significant cyber-attack, like the NotPetya malware incident in 2017,[39] a firm may not have access to IARD to provide a report and may not want to use any form of electronic filing if it is suspected that bad actors remain in a potentially compromised system. By contrast, the Banking Rule provides the option for registered entities to provide notification through alternative secure means, including by phone.

Harmonization with other regulatory requirements will reduce unnecessary compliance burdens and will maximize an organization's ability to focus on protecting clients and investors in a crisis and restoring the confidentiality, availability, and integrity of information systems. To that end, the Commission may also consider borrowing elements from other regulatory notification standards. For example, the Federal Reserve Bank's Operating Circular No. 5 (OC 5) builds a notice requirement around an "impact" analysis that focuses on the effects of an event rather than

[33] We imagine that a firm and the Commission could continue to communicate informally in between providing an initial notice and submitting a final incident report.
[34] 87 Fed. Reg. 13592.
[35] 86 Fed. Reg. 66424.
[36] *Id.* at 66433.
[37] *Id.*
[38] *Id.*
[39] *See* Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

the root cause or the immediate IT aftermath.[40] We also observe that FINRA has taken an effective approach to investigating cyber-attacks.[41]

(2) **Notice should be triggered upon an institution's "determination" of a significant cybersecurity incident, which would provide a clear notification standard and align with the Banking Rule and the Commission's proposed rules on public company cybersecurity disclosures.**

We recommend the Commission allow for notification after advisers "determine" that a significant cybersecurity incident has occurred. Under proposed rule 204-6, advisers must report significant cyber incidents within 48 hours after having a "reasonable basis to conclude that any significant adviser or fund cybersecurity incident has occurred or is occurring with respect to itself or any of its clients that are covered clients."[42] We appreciate that the Commission specifically seeks comment on whether the "reasonable basis" standard is clear,[43] and we respectfully observe that it is not. In our view, the "reasonable basis" standard can only be properly evaluated in hindsight, after all the incident facts become known. Incorporating this language into the notice trigger would only serve to confuse—not clarify—advisers' understanding of when notice should be provided. During the haze of an emergent cyber disruption, which could roll across different segments of the same network at different times, it is difficult, if not impossible, to assess exactly when it is reasonable to conclude that the disruption has evolved into a clear notification-triggering incident. We assume the Commission understands that, in the first critical hours and days of a cybersecurity incident, advisers will be focused on mitigating the intrusion and understanding the scope of the attack. Once it is determined, based on that information, that an incident meets the reporting standard, the 48-hour clock should start. Attaching notification to a clearer "determination" standard would provide clarity and would help avoid unnecessary reporting of insignificant cyber intrusions, which may not ultimately affect the security or integrity of personal or sensitive information.

A revised "determination" threshold would again align the Commission's notice obligation with that of the Banking Rule, which requires a banking organization to notify its primary federal regulator of a "computer-security incident" that rises to the level of a "notification incident" after the organization "determines that a notification incident has occurred."[44] In fact, the OCC, Federal Reserve, and FDIC revised the original proposed rule, which required notification after an organization "believes in good faith that a notification incident has occurred"[45] following pushback from commentators.[46] According to the agencies, the "[u]se of the term 'determined' allows the

[40] *See* Federal Reserve Bank's Operating Circular No. 5 (OC 5) (effective June 30, 2021), § 1.4 ("Institution's Security Obligations").
[41] One member reports that FINRA has made it clear that it works around a firm's schedule of investigating and resolving an incident rather than insisting on conducting interviews while the firm works toward remediation.
[42] 87 Fed. Reg. 13537.
[43] *See id.* at 13538 (Comment Request #41).
[44] 86 Fed. Reg. 66427.
[45] Notice of Proposed Rulemaking, Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 2302.
[46] 86 Fed. Reg. 66434.

bank service provider time to examine the nature of the incident and assess the materiality of the disruption or degradation of covered services."[47]

A "determination" standard would also align with the Commission's recently proposed rules on public company cybersecurity disclosures.[48] In those proposed rules, the Commission has established that a Form 8-K disclosure requirement is triggered when a registrant "determines" that it has experienced a material cybersecurity incident.[49]

We also appreciate the request for comment regarding whether the Commission should require that a particular person be responsible for "gathering relevant information about the [significant cybersecurity] incident and having a reasonable basis to conclude that such an incident occurred."[50] In our view, any such requirement would amount to unreasonable overreach and micromanagement, and we respectfully ask the Commission to exclude any obligatory designation from a potential final rule. Our member firms have unique internal processes for assessing the materiality of any incident, regardless of the type. In many cases, these processes do not fall on one specific person but rather involve specific committees or subcommittees that are focused on cybersecurity issues. An institution should be permitted to employ its own established processes to determine whether a significant cybersecurity incident has occurred. If the Commission would like to inquire about that process, it can do so, but it should not prescribe any intra-firm regulation.

(3) **An exemption for adverse harm must be incorporated into the proposed reporting regime.**

In certain, limited circumstances, reporting itself could result in significant broader adverse harm, and the proposed regime should provide highly confidential reporting and express delays for these circumstances where a report, if made public, could result in broader adverse harm. As an example, if a zero-day vulnerability or exploit in a product or information system is discovered by a regulated entity, the entity should have an opportunity to notify the vendor of the product or information system so that vendor has an opportunity to develop a patch that can be issued before the vulnerability or exploit becomes more widely known. Such a "responsible disclosure" exception would allow vendors a reasonable opportunity to develop a patch so that other companies could harden their cyber defenses and eliminate the possibility that a report under this regime could alert hackers to an unpatched weakness and lead to a more widespread harm than otherwise would have been experienced.

(4) **A law enforcement exemption must be incorporated into the proposed reporting regime.**

State data breach statutes generally include an omnibus law enforcement exception: at the request of law enforcement, institutions may withhold information from attorneys general and data subjects until the conclusion of a particular investigation. We observe that the Commission did not build that standard into the proposed reporting requirement, and we respectfully request that the

[47] *Id.*
[48] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11038, 34-94382, IC-34529, 87 Fed. Reg. 16590 (to be codified at 17 C.F.R. pts. 229, 232, 239, 240, 249).
[49] *Id.* at 16595.
[50] 87 Fed. Reg. 13537 (Comment Request #37).

Commission consider doing so. Such an exception should be triggered if an adviser or fund is actively working with law enforcement or the intelligence community on an investigation and law enforcement has indicated in writing that delay of reporting would facilitate enforcement goals. It is hard to imagine the Commission would want to risk exposing an ongoing federal criminal or intelligence investigation into a hacking incident in order to start an investigation of whether the attacked institution had adequate security or adequately disclosed the risk of an attack.

However, we also observe that this exception might not be necessary if the Commission adopts our proposed initial notification method. Notifying the Commission of an emergent cyber issue through a phone call, email, or appropriate discreet channel can occur while an institution is simultaneously cooperating with law enforcement. We note that the issue of a law enforcement exception surfaces when an institution is compelled to file a more formal report in the middle of an active law enforcement investigation.

(5) Parent financial institutions should be permitted to file on behalf of affected subsidiary advisers.

As currently proposed, rule 204-6 does not specify that related advisers in the same corporate family can file a single report concerning the same significant cybersecurity incident. We believe that such a provision must be included in a potential final rule and observe that the Commission already permits a form of linking for affiliates for disciplinary matters between broker-dealers and their advisory affiliates. Large organizations have many advisers,[51] and different legal or compliance personnel often manage the filings of these advisers. Depending on the scope of the cybersecurity incident, these organizations could also be subject to numerous notice requirements managed by different functions. It would be unnecessarily burdensome—for both the advisers and the Commission—to require related advisers in the same corporate family to file multiple identical notices about the same event.

If a significant cybersecurity incident affects multiple branch advisers, only one office should be required to notify the Commission and subsequently provide a potential report. This system would benefit institutions, which would save time and preserve resources by providing streamlined notice, avoiding redundant reporting, as well as the Commission, which would receive the data it seeks without being inundated with multiple identical accounts of the same matter.[52]

[51] One member has more than 20 registered investment advisers.
[52] We note, however, that related entities should not be compelled to coordinate reporting.

vi. **The Commission should revise definitions to prevent over reporting and align with language in Regulation S-P and the Commission Statement and Guidance on Public Company Cybersecurity Disclosures ("2018 Interpretive Release").**[53]

(1) **The Commission should change its definitions of "personal information" and "adviser information" to prevent over reporting and align with definitions in Regulation S-P.**

We observe that the proposed definition of "personal information," which is only loosely tied to the Commission's broad concept of "cybersecurity incident," deviates from the Commission's definition of personal information in Regulation S-P and would, as currently drafted, unnecessarily capture trivial transactional data. For incident reporting, "adviser information" is proposed to be defined as "any electronic information related to the adviser's business, including personal information, received, maintained, created, or processed by the adviser."[54] The term "personal information" is, in turn, proposed to be defined as: "(1) any information that can be used, alone or in conjunction with any other information, to identify an individual, such as name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, driver's license number, electronic mail address, account number, account password, biometric records or other *non-public authentication information*; or (2) any other non-public information regarding a client's account" (emphasis added).[55]

We appreciate the fact that the Commission's definition of "personal information" for advisers and funds is derived from "established sources" intended to capture a broad range of data that can reside in an adviser's or fund's systems.[56] Nevertheless, we observe that under the Commission's current concept of nonpublic authentication information, inconsequential transactional authentication information—i.e. the name of a user's first pet—could potentially become notification-triggering personal information. Moreover, the rule's proposed definition of personal information deviates from the industry-standard definition set forth in the Gramm–Leach–Bliley Act ("GLBA") and adopted by the Commission's Regulation S-P. We recommend that the Commission harmonize the proposed rule's concept of personal information with that of Regulation S-P and accordingly use the term "nonpublic personal information" defined as "(i) personally identifiable financial information; and (ii) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available information."[57]

---

[53] *See* 17 C.F.R. pt. 248; Commission Statement and Guidance on Public Company Cybersecurity Disclosures ("2018 Interpretive Release"), Release No. 33-10459, 83 Fed. Reg. 8166.
[54] 87 Fed. Reg. 13592-93.
[55] *Id.* at 13539 n.31.
[56] *Id.*
[57] 17 C.F.R. pt. 248.3(t)(1). Under Regulation S-P, "personally identifiable financial information" means "any information: (i) a consumer provides to you to obtain a financial product or service from you; (ii) about a consumer resulting from any transaction involving a financial product or service between you and a consumer; or (iii) you otherwise obtain about a consumer in connection with providing a financial product or service to that consumer." 17 C.F.R. pt. 248.3(u)(1).

Additionally, to the extent the Commission is wed to incorporating the concept of "[nonpublic] personal information" into a definition of "adviser information," we suggest the Commission tailor the definition of "adviser information" to include only "[nonpublic] personal information, received, maintained, created, or processed by the adviser," striking the first part of the proposed definition: "any electronic information related to an adviser's business." As currently drafted, the definition of adviser information is overly broad and would, for example, encompass even a business address.

(2) **The Commission should amend its definitions of "significant adviser/fund cybersecurity incidents" and implement a materiality standard in line with the 2018 Interpretive Release and its proposed rules on public company disclosures.**

The Commission proposes to define a notification-triggering significant adviser cybersecurity incident as a "cybersecurity incident, or a group of related incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: (1) Substantial harm to the adviser, or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed."[58] As discussed herein, we have concerns about this proposed definition and appreciate the opportunity to put forth suggested revisions.

As an initial matter, we emphasize that a final definition of significant cybersecurity incident must require notification of only those incidents involving *actual harm*. Again, this would align the Commission's reporting requirement with that of the Banking Rule, which defines a "computer-security incident" as an "occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits."[59] An actual-harm standard would ensure that institutions are not compelled to report harmless cyber intrusions at the expense of directing resources toward incident response. Relatedly, we believe that the word "degrades," as currently used in the definition, is unclear, overbroad, and would ultimately capture unnecessary cyber incidents; to that end, we propose the Commission eliminate the term from a final definition of significant cybersecurity incident.

The Commission requests comment on whether the "substantial harm" threshold for "significant adviser cybersecurity incidents" and "significant fund cybersecurity incidents" is appropriate.[60] As noted above, the second prong of the proposed definition of "significant adviser cybersecurity incident" includes a cybersecurity incident that leads to "unauthorized access or use of adviser information resulting in (1) substantial harm to the adviser or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed."[61] Similarly, the second prong of "significant fund cybersecurity incident" includes a cybersecurity incident that "leads to the

[58] 87 Fed. Reg. 13536. As we previously noted, this definition is "substantially similar" to the proposed definition of significant fund cybersecurity incident. *Id.* at n.60.
[59] 86 Fed. Reg. 66442. Notably only those computer-security incidents that fall within the definition of "notification incident" are required to be reported under the Banking Rule. *Id.* at 66429.
[60] 87 Fed. Reg. 13538 (Comment Request #40).
[61] *Id.* at 13536.

unauthorized access or use of fund information, which results in substantial harm to the fund, or to the investor whose information was accessed."[62]

As the Commission notes, substantial harm to an adviser or client could include "significant monetary loss or theft of intellectual property," while substantial harm to a client or an investor in a private fund (as the result of an incident in which adviser information is compromised) may include "significant monetary loss or the theft of personally identifiable or proprietary information." [63] Though the Commission does not appear to further clarify substantial harm in the context of notice-triggering fund incidents, it does state that significant fund cybersecurity incidents may include "cyber intruders interfering with a fund's ability to redeem investors, calculate NAV or otherwise conduct its business."[64]

We appreciate the Commission's short list of examples of substantial harm and significant fund cybersecurity incidents but believe that the current substantial harm threshold is too broad and appears to deviate from the "materiality" standard set forth in the 2018 Interpretive Release. In the 2018 Interpretive Release, the Commission states that public companies must take "all required actions to inform investors about *material* cybersecurity risks and incidents in a timely fashion, including those companies that are subject to *material* cybersecurity risks but may not yet have been the target of a cyber-attack" (emphasis added).[65] As referenced above, the Commission has also adopted a materiality standard for its proposed rules on cybersecurity on public company cybersecurity disclosures.[66] As such, we request that the Commission harmonize its proposed adviser/fund definitions with both existing guidance and with its public company rule proposals and use the "materiality" measuring stick it has in place.

Additionally, we believe that the second prong of "significant adviser/fund cybersecurity incidents" would capture potentially immaterial matters. For example, as currently drafted, without an additional modifier or materiality threshold, the proposed definition suggests that an adviser must report an incident that may only affect a single client of a single fund. Further, the Commission's definition of "significant adviser cybersecurity incident" seems to suggest that advisers have an obligation to report incidents impacting private fund clients regardless of the involvement of the adviser's information systems. As currently proposed, this is unworkable as an adviser is highly unlikely to have necessary information to make a report and should not be responsible for private fund clients' information technology systems.

A significant timing problem also exists: in the fog of an unfolding cybersecurity incident, one may not know if "substantial harm" has even occurred until after the incident is resolved or data is analyzed. For instance, a hacker who is able to encrypt a server with ransomware may or may

---

[62] *Id.* at 13537.
[63] *Id.* at 13536-37.
[64] Other significant fund cybersecurity incidents may involve the "theft of fund information, such as non-public portfolio holdings, or personally identifiable information of the fund's employees, directors or shareholders." *Id.* at 13537.
[65] 2018 Interpretive Release, *supra* note 53, at 4.
[66] *See* 87 Fed. Reg. 16590 ("Specifically, we are proposing amendments to require current reporting about material cybersecurity incidents… The proposed amendments are intended to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents.").

not have been able to take data from that server before encryption, and whether that data poses any harm, much less substantial or material harm, could often entail weeks of data mining.

We urge the Commission not to follow the path of the EU's General Data Protection Regulation ("GDPR"), which has left the Data Protection Authorities flooded with data breach notices.[67] To that end, we request that the Commission revise the second prong of "significant adviser/fund cybersecurity incidents" to ensure that the definition is consistent with other SEC frameworks and does not lead to unnecessary immaterial notifications.

vii. Incident reporting must remain confidential, and the Commission must ensure that provided information is protected.

We appreciate and support the Commission's decision to keep reporting confidential. To that end, we request that any reporting information be exempt from Freedom of Information Act ("FOIA") requests and any other freedom-of-information laws that could potentially compel disclosure. This exemption would align with the FOIA carve-out in the recently signed CIRCIA legislation.[68]

We also request that the Commission include in the finalized rule more robust language about how it will protect confidential data from being leaked to threat actors or members of the press.[69]

As expressed above, without more insight into the Commission's policies and procedures for safeguarding sensitive information in its presumably centralized database, we are hesitant to provide proprietary or risk-related data. If the Commission is unable to adequately ensure that information will be properly safeguarded, we recommend that firms have the option to maintain their own cyber records—in a federated system that is not a high-value target for bad actors—and permit the Commission to examine that information onsite.

We also encourage the Commission to consider ways to work with federal law enforcement and other regulators and ensure timely sharing of threat intelligence information regarding ongoing

---

[67] *See* Catherine Stupp, *European Privacy Regulators Find Their Workload Expands Along with Authority*, Wall St. J. (April 12, 2019 7:44 AM), https://www.wsj.com/articles/european-privacy-regulators-find-their-workload-expands-along-with-authority-11555061402 ("European regulators are struggling to keep up with the big increase in corporate data breach notifications since the European Union privacy law took effect…Much of the workload stems from a requirement under the General Data Protection Regulation for companies to inform regulators within 72 hours after they suffer a breach of personal data. Companies are struggling to understand what qualifies as a breach that they must report to authorities."); Eline Chivot, Opinion, *One Year On, GDPR Needs A Reality Check*, FINANCIAL TIMES (June 30, 2019), https://www.ft.com/content/26ee4f7c-982d-11e9-98b9-e38c177b152f (noting that since the GDPR has been enacted, data protection authorities in the UK and France have admitted they are "overwhelmed by a flood of companies reporting themselves for violations" and suggesting the EU should offer better guidance on breaches).

[68] *See* CIRCIA, *supra* note 6 ("Reports describing covered cyber incidents or ransom payments submitted to the Agency by entities in accordance with section 2242, as well as voluntarily-submitted cyber incident reports submitted to the Agency pursuant to section 2243, shall…be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the 'Freedom of Information Act'), as well as any provision of State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records…").

[69] *See, e.g.*, SIFMA Data Protection Principles (March 2021), *available at* https://www.sifma.org/wp-content/uploads/2017/11/SIFMA-Data-Protection-Principles-March-2021.pdf (establishing overarching best practices for the protection of sensitive data that aligns to the Cyber Risk Institute Financial Sector Profile and the NIST Cybersecurity Framework).

attacks in a manner that shares actionable information while maintaining the confidentiality of identified information from competitor firms.

4. Disclosure Requirements Regarding Cybersecurity Risks and Incidents

a. Overview of Proposed Amendments to Form ADV Part 2A, Proposed Amendments to Rule 204-3(b) of the Advisers Act, and Proposed Amendments to Fund Registration Statement Forms

The Commission proposes amendments to adviser and fund disclosure requirements to provide current and prospective clients and shareholders with "improved information" regarding cybersecurity incidents and risks.[70] Specifically, the Commission proposes amendments to Form ADV Part 2A for advisers that would add a new Item 20 entitled "Cybersecurity Risk and Incidents" to the form's publicly available narrative brochure. Amended Form ADV Part 2A would, in short, require disclosure of cybersecurity risks as well as certain significant cybersecurity incidents occurring within the last two fiscal years. Additionally, the Commission has proposed to amend rule 204-3 (b) of the Advisers Act to require advisers to promptly deliver interim brochure amendments or supplements to existing clients if the adviser "adds disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed in its brochure about such an incident."[71] A fund would be required to disclose in its registration statement whether a significant fund cybersecurity incident has affected or is currently affecting the fund or its service providers. A fund would also be required to disclose this information regarding any significant fund cybersecurity incident occurring the last two years. Additionally, a fund would be required to update its prospectus by filing a supplement with the Commission. The Commission proposes amendments to Forms N-1A, N-2, N-3, N-4, N-6, N-8B-2, and S-6 for funds.

b. Discussion of Comments on Proposed Amendments to Form ADV Part 2A, Proposed Amendments to Rule 204-3(b) of the Advisers Act, and Proposed Amendments to Fund Registration Statement Forms

The Commission observes that new cyber-related disclosure requirements would "enhance investor protection by requiring that cybersecurity risk or incident-related information is available to increase understanding in these areas and help ensure that investors and clients can make informed investment decisions."[72]

We support the Commission's attempt to foster greater adviser and fund transparency regarding cybersecurity preparedness, including the existence of policies and procedures to detect, defend against, and respond to cybersecurity incidents, and believe that investors and shareholders deserve a clear understanding of a firm's posture in these respects. Notably, public companies have certain disclosure obligations regarding issues that may be material to investors, and private investors deserve similar information (that can include cybersecurity matters if, for example, customer data was stolen or a ransomware payment was made).

[70] 87 Fed. Reg. 13527.
[71] *Id.* at 13540.
[72] *Id.* at 13527.

While we support the goals of cybersecurity preparedness and transparency, we oppose any requirement that compels burdensome continuous public disclosure of detailed information relating to cybersecurity incidents or risks and offer suggestions to revise the Commission's proposed new cyber disclosure regime.

i. **The proposed disclosure requirements are unduly burdensome for advisers and funds and must be amended to be workable for our members.**

We respectfully urge the Commission to reconsider its proposed disclosure obligations, particularly its suggested vehicles for disclosure (amended Form ADV Part 2A brochure and the fund prospectus) given the significant burdens and costs associated with delivering such brochures, brochure supplements, and prospectuses. Further, advisers should not be required to continually update or revise disclosures and funds should not be compelled to publicly disclose a cybersecurity incident currently affecting it or file a prospectus supplement with the Commission.

For advisers, the Commission proposes an amendment to rule 204-3(b) that would require an adviser to deliver interim brochure amendments to existing clients promptly if the adviser adds disclosure of a cybersecurity incident to its brochure or "materially revises" information disclosed in its brochure about such an incident.[73] New Item 20.B would require disclosure of cybersecurity events that meet the definition of a significant adviser cybersecurity incident and the information required corresponds to the information requested on Form ADV-C, though at a more general level. We observe that most information requested in response to Item 20.B could easily be provided in a fill-in-the-blank or check-the-box format, with the exception of a narrative response describing the effect of the incident on the adviser's operations. As the information required to be disclosed more closely aligns with a form-style of disclosure, requiring narrative disclosure within Part 2A of Form ADV is simply not appropriate.

The Commission may have overlooked some cost and resource burdens advisers would have to undertake to deliver amended brochures or a summary update to clients, for each initial and updated significant cybersecurity event. When updating Part 2A of Form ADV, an adviser must typically draft the disclosure, prepare the amended document for printing, update and post electronic files to internal and external websites, print amended documents and the summary of the changes, and mail or email the notifications to clients. The time, effort, and cost associated with each amendment is significant. For a conservative "pre-planned" scenario where drafting and preparing takes minimal effort and notification to clients may be incorporated into a planned upcoming communication such as a client statement, the cost per update is approximately $50,000. For an "ad hoc unplanned" scenario, meaning the client notification and update cannot be combined with a planned upcoming client communication, the cost per update rises significantly. A firm with a mailing to 500,000 clients would have the additional cost of the envelope, paper, and postage of approximately $1.00 per client. In this scenario, the cost per update is approximately $550,000.

We urge the Commission to consider other publicly available methods of disclosure, such as existing form-styles of disclosures, that are easier to complete and less costly. We also

[73] *Id.* at 13540.

recommend that the Commission only require advisers to update cybersecurity disclosures or deliver brochure amendments on an annual basis and emphasize again that the burden and operational cost of multiple filings for a single event is significant given that delivery to clients is resource intensive.

From a fund perspective, we observe, as an initial matter, that the proper document for disclosure is the *annual report* and not the fund prospectus.

Funds should not be required to publicly disclose a significant cybersecurity incident that is currently affecting the fund. Such a real-time disclosure requirement is unduly burdensome and risks diverting incident response resources to the disclosure and communications process.

To provide timely disclosures of cybersecurity risks and significant fund cybersecurity incidents, the Commission proposes that a fund amend its prospectus by filing a supplement with the Commission. We are concerned about the high cost of doing this, as well as the fact that the provided information could quickly become public, presenting an opportunity for further exploit by bad actors and others.

Cybersecurity intrusions are dynamic, and continual client updates could function to confuse clients, as these updates are not likely to provide information that clients find particularly meaningful or helpful as incidents unfold. Additionally, clients may not have the necessary context or expertise to act on frequently revised information, which could result in disclosures being unnecessarily harmful to both the firm and financial markets.

ii. **Advisers should have the option to disclose information to clients electronically.**

We strongly urge the Commission to adopt electronic methods of delivery and notification, such as posting information to a secure website accessible to clients.[74] The Commission has recently adopted many methods and formats of electronic disclosure, either by email or posting to websites. We also strongly urge the Commission to adopt an electronic disclosure format that allows advisers to make cybersecurity disclosures available to clients in a manner that is cost effective and less labor intensive to update. We believe electronic disclosure formats promote the Commission's goal of keeping investors informed and allows advisers to provide information on a timely basis.

iii. **To the extent the Commission includes a lookback period in the finalized rules, that period must be shortened to twelve months.**

We appreciate the request for comment on the two-year lookback period for cybersecurity incident public disclosures. We question the value of disclosing to shareholders cyber incidents that have occurred in the past, particularly given the rapid evolution of cyber threats, and accordingly

[74] While electronic delivery of notices should be the default, we ask the Commission to retain a paper option for all disclosures. In particular, certain state data breach disclosure laws require paper notifications, and there is no reason to duplicate notices and confuse recipients.

recommend the Commission eliminate the lookback term. If such a period does appear in the final rule, we respectfully request that it be shortened from two years to twelve months.[75]

Moreover, we ask the Commission to keep in mind that, if adopted, this will be a new requirement and not every firm is currently maintaining the necessary relevant data points that go back two years (or even one year) and request that the Commission provide some leniency in this regard. The burden of these sorts of complex retrospective requirements could be particularly complex for large firms that are frequently adding or subtracting business units.

iv. The Commission should not require disclosures regarding service providers.[76]

The proposed disclosure amendments would require that a fund disclose to investors in its registration statement whether a significant fund cybersecurity incident has or is currently affecting the fund or its service providers. We believe that the final rule must take into account the realities of federated operating models with externally hosted platforms that many funds have little control over, especially if it is a larger service provider with greater bargaining power.

Even substantial firms have essentially no ability to negotiate terms with large companies, yet these firms frequently offer some of the most robust, redundant, and professional information security. It would be counter-productive to require some pervasive oversight that results in an adviser not being able to benefit from top-tier cloud providers and having to rely upon perhaps less-secure mid-market cloud providers willing to provide the sort of reporting that the Commission requires. We fear that funds will not be able to renegotiate contracts with some service providers, and in the context of cloud-service providers, this may ultimately result in driving funds away from more-secure cloud platforms and back into on-premise servers, which would generally diminish cybersecurity.

The integration of third-party service providers into disclosure requirements will only magnify these issues. We suggest the Commission review the recent data breach at the otherwise well-regarded cloud provider NetGain. That provider discovered anomalous network activity in November 2020, though it took until the end of February 2021 for the company to determine that

[75] The Commission has previously shortened lookback periods in final rulemaking decisions. For example, when the Commission adopted final amendments to certain auditor independence requirements in Rule 2-01 of Regulation S-X, it shortened the lookback period for an auditor's independence assessment to one year from the previous rule that required a lookback period of two or three years for U.S. companies. *See* Qualifications of Accountants, 17 CFR 210, Release No. 33-10876; 34-90210, *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[76] In its discussion of cybersecurity risk management policies and procedures, the Commission proposes that advisers and funds assess the compliance of "all service providers that receive, maintain, or process adviser or fund information, or are otherwise permitted to access adviser or fund information systems and any adviser or fund information residing therein." 87 Fed. Reg. 13533 (Comment Request #14). As we discuss in section 5(b)(ii) of this letter, the Commission should narrow this set of service providers to exclude adviser/fund affiliates, including only certain "named service providers" defined at 87. Fed. Reg. 13526. To the extent the Commission insists that some level of disclosure from regulated service providers is necessary, we respectfully ask that such a requirement apply only to certain "named service providers," excluding firm affiliates.

the activity was indeed a ransomware attack.[77] Further, it took another five months for NetGain to complete a forensic investigation and sort out exactly which of its clients' data was impacted and to what degree.[78] If a large service provider were to be exposed to a sophisticated malware, such as what was present in the SolarWinds attack, the entity may not know the extent of the attack for a considerable period of time.

v. The Commission should clarify that a summary of an incident that does not compromise an ongoing remediation is sufficient for client disclosure purposes.

The Commission proposes to require a robust vulnerability management program be in place to monitor, detect, and respond to identified vulnerabilities, which certainly seems prudent. We respectfully ask the Commission, however, that this program not require disclosures of vulnerabilities that could lead to threat actors obtaining a roadmap that may assist in the planning and execution of future cyber-attacks. Publicly disclosing vulnerabilities provides attackers with a wealth of easily exploitable information about a firm's system and data residing therein. Given the lifecycle of a vulnerability, it does not make sense to provide such information to the Commission. A vulnerability does not pose risk unless it is known, and increased reporting of vulnerabilities will serve to increase dissemination of the risk.

We accordingly suggest that the proposed description of disclosed cybersecurity incidents include only limited facts with specific details about neither the specific techniques nor the tactics used in successful attacks nor the effect of the incident on business operations or about remediation efforts.[79] At a minimum, the disclosure of vulnerabilities should be significantly delayed until after the company that owns or manages the product or information system with the vulnerability has been notified and had an opportunity to provide a patch to the market.

5. Cybersecurity Risk Management Rules

a. Overview of Proposed Rule 206(4)-9 under the Advisers Act and Proposed Rule 38a-2 under the Investment Company Act

The Commission proposes cyber risk management rules that would require advisers and funds to implement cybersecurity policies and procedures that are "reasonably designed" to address cybersecurity risks.[80] The proposed rules set forth elements that advisers and funds would need to include in their policies and procedures, with the Commission allowing covered entities to "tailor their cybersecurity policies and procedures to fit the nature and scope of their business and address their individual cybersecurity risks."[81] These elements include an assessment of the fund's risks,

---

[77] *See* Jonathan Greig, *Healthcare Orgs in California, Arizona Send Out Breach Letters for Nearly 150,000 after SSNs Accessed During Ransomware Attacks*, ZDNET (Sept. 10, 2021), https://www.zdnet.com/article/healthcare-orgs-in-california-arizona-send-out-breach-notice-letters-for-nearly-150000-after-ssns-accessed-during-ransomware-attacks.

[78] *Id.*

[79] We also emphasize that the Commission should not require advisers to report or disclose incidents suffered by clients. Such a requirement assumes that an adviser/fund will be made aware of such incidents in a timely manner. It also imposes additional obligations on a firm where the firm's information and information systems may not be affected in any way, and where the adviser/fund is in compliance with the rules.

[80] 87 Fed. Reg. 13528.

[81] *Id.*

controls to prevent unauthorized access to systems and information residing therein, a threat and vulnerability management regime, and an incident-response plan detailing the mechanisms to ultimately mitigate a breach. Additionally, the Commission proposes board of director oversight requirements for funds, annual adviser reviews assessing the design and effectiveness of cybersecurity policies and procedures, and various new recordkeeping obligations.

b. Discussion of Comments on Proposed Rule 206(4)-9 under the Advisers Act and Proposed Rule 38a-2 under the Investment Company Act

The Commission observes that the proposed risk management rules would "help address operational and other risks that could harm advisory clients and fund investors or lead to the unauthorized access to or use of adviser or fund information."[82] While we support the purpose of robust cyber hygiene rules, flexibility is vital.

The Commission should adopt a principles-based approach to risk management, as opposed to a system of policy and control prescriptions that would undermine the Commission's accurate observation that there is no "one-size-fits-all" solution to data privacy and cybersecurity.[83]

As such, we respectfully put forth recommendations that would amend the Commission's proposed cyber risk management rules to ensure that advisers and funds can indeed "tailor their cybersecurity policies and procedures based on their individual facts and circumstances" and "varying characteristics."[84]

i. While the Commission should continue to recommend risk-management best practices, it should not mandate the implementation of specific security measures or controls.

We agree that the ubiquity of cybercrime should induce institutions to invest in data protection and cybersecurity but observe that firms build security programs in different ways to address different cyber concerns. A large firm with institution-wide security policies and capabilities may approach risk quantification and vulnerability management in a manner distinct from the approach of a small fund with fewer resources and possibly different threat concerns. Some institutions have completely implemented one of the cybersecurity frameworks referenced by the Commission, while others have built cyber programs by taking components from several frameworks based on a comprehensive risk assessment. Still others have bespoke approaches consistent with unique architectural requirements that are best validated through testing.

For large firms with advisers and funds subject to other regulatory regimes, it would be unnecessarily onerous to have a separate administrative process related to compliance solely specific to these proposed rules when comprehensive risk management programs are already in place. We wish to ensure that the proposed rules are workable for our members with a complex legal entity structure of advisors and other investment company affiliated service providers who rely on centralized institutional functions to provide cybersecurity and technology controls. To that end, we believe that further consideration should be given to the ways in which the

[82] *Id.*
[83] *Id.* at 13527.
[84] *Id.* at 13528.

Commission's proposals might challenge this model. We emphasize that cyber regulation should be threat-informed and risk-based, as well as flexible to account for factors such as different business models, the size of the adviser's and fund's assets under management, nature of operations, revenue, and available institutional resources. For example, the proposed rules require "measures to detect, mitigate, and remediate *any* cybersecurity threats and vulnerabilities with respect to [adviser/fund] information systems and the [adviser/fund] information residing therein" (emphasis added).[85] We note that the requirement to remediate any vulnerability ignores a firm's consideration of whether that vulnerability is high-risk in light of its IT environment; moreover, many firms already have in place risk-based policies and standards for vulnerability assessment and remediation.

We highlight two areas of gratuitous prescription and request the Commission clarify that any specified measures or controls be adopted only on a discretionary basis. It is our view that the Commission should avoid prescribing a particular cybersecurity regime and instead ensure firms focus on best practices commensurate with risk.

(1) The Commission's proposed risk assessment, based on an implicit inventory requirement, is overly burdensome and should be amended.

The proposed cyber policy and procedure rules require a risk assessment that involves the categorization and prioritization of risks "based on an inventory of the components of their information systems, the information residing therein, and the potential effect of a cybersecurity incident on the advisers and funds."[86] This implicit inventory requirement would be particularly challenging to enact given the Commission's broad definitions of adviser/fund information and information systems. The proposed definition of adviser/fund information includes "any electronic information related to the [adviser's or fund's] business, including personal information, received, maintained, created, or processed by the [adviser/fund]."[87] Meanwhile the Commission has proposed to define adviser/fund information systems as "the information resources owned *or used* by the [adviser or fund], including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of [adviser/fund] information to maintain or support the [adviser's or fund's] operations" (emphasis added).[88] Given the breadth of these definitions—as well as the expansive definition of personal information—an inventory of information systems would ultimately cover most operations of a firm, not just those that are pertinent to providing investment services.[89] Requiring advisers and funds to inventory all of these components and information sources would be unduly burdensome and create unreasonable expense.

---

[85] *Id.* at 13588, 13593.
[86] *Id* at 13529.
[87] *Id.* at 13589, 13593.
[88] *Id.* at 13589, 13593. The Commission notes that for the risk management policies and procedures, the proposed defined terms for advisers and funds are the same in most instances and that "the majority of differences between proposed rules 206(4)-9 and 38a-2 are that the rule applicable to advisers includes the word 'adviser' in a number of terms (*e.g.*, 'adviser information systems' and 'adviser information') whereas the rule applicable to funds includes the word 'fund' (*e.g.*, 'fund information systems' and 'fund information.')." *Id.* at 13528 n.25.
[89] We observe that the definitions of information systems should explicitly exclude third party information systems.

Inventories can and should be focused on the overall architecturally significant components of systems and devices on networks, as opposed to the data on particular devices. The cost of achieving a constantly, self-refreshing inventory of all data is disproportional to its benefit; if data is to be inventoried, the requirements should extend only to the identification of material databases. The Commission simply assumes without any cited support that the assessment of risks must begin with a detailed inventory. Although some general knowledge of the material elements of the systems, network, architecture, and data is required, a detailed inventory is not. The Commission cites no evidence and we are not aware of any (other than the marketing of software companies) to the effect that spending large amounts on continually evolving inventories will result in better security that justifies the associated administrative costs.

Unstructured data sets, such as emails or Word documents, should be excluded from any detailed inventory requirements. The cost and effort to develop an inventory of unstructured data would be disproportionate to any cybersecurity benefit, as attackers normally would not be willing or able to spend the resources necessary to parse such data. We accordingly suggest that any recommendation be limited to devices (and not include data) in order to minimize the burdens associated with compiling a risk assessment.

While it may be helpful and even good practice to create a detailed inventory, it should in no way be a requirement to commence a risk assessment.

Further, any risk assessment should be periodic and determined by the entity based on its size, business model, and sensitivity of the data in scope. We also emphasize that any required components that would form a risk assessment be limited so that institutions can maintain flexibility to address cybersecurity risks unique to their operations. For example, a fund that relies on third-party IT infrastructure may have more elements focusing on third-party due diligence and assurances than an adviser that primarily operates its own IT infrastructure. Moreover, as noted above, flexibility is needed so that covered advisers or funds may rely on the risk assessments, and overall cybersecurity programs, of parent companies.

(2) The Commission should not compel firms to implement specific controls, including multi-factor authentication ("MFA").

The Commission notes that an adviser's or fund's policies and procedures "must include" certain controls, such as "identifying and authenticating individual users, including implementing authentication measures that require users to present a combination of two more credentials for access verification" (commonly known as MFA).[90] While we recognize the benefits of MFA—and the fact that many firms have successfully incorporated it into current cyber programs—the Commission should avoid implementing blanket security control prescriptions.[91] To the extent a

[90] 87 Fed. Reg. 13530. Additionally, the Commission appears to require the incorporation of least-privilege principles into adviser/fund policies and procedures.

[91] Similarly, we request that the Commission exclude penetration tests from a potential recommended list of security practices. *See id.* at 13531. While we recognize that penetration testing can be a useful control for some purposes and is requested by other regulators, it is nonetheless a point-in-time assessment of a firm's systems that may not be the best barometer of overall security. We note that our member firms are exploring more effective ways of obtaining

final rule includes any cyber program requirements or best-practice recommendations, entities should be able to implement those measures in accordance with their internal risk assessment and evolving authentication technology that could, in the future, supplant MFA as a current best (or better) practice; otherwise, the requirements will be too prescriptive.[92]

The application of MFA and other controls should be consistent with a firm's risk assessment; for example, many firms use MFA to gain access to their corporate network, and then rely on single sign-on "handshakes" to access business applications inside the network. Moreover, given the rapid evolution of the cyber threat environment, as well as defensive technologies and tooling, controls such as MFA should not be mandated. For example, the FBI and CISA recently released a joint Cybersecurity Advisory (CSA) to warn organizations that Russian state-sponsored cyber actors have gained network access through exploitation of default MFA protocols and a known vulnerability.[93] Because of the rapidly changing nature of technology, specific requirements like MFA should not be mandated, because they could quickly become outdated. Instead, a requirement to have a processes and procedures would satisfy this need, along with a publication of best practices that firms can choose to adopt based on specific circumstances. What the Commission may mandate this year in terms of security controls can become completely obsolete by the following year.

We observe that if the Commission is going to require some form of risk assessment, then it should respect that assessment: in other words, it should allow firms to use any evaluation of risk as a way to discern whether certain measures and controls are necessary to adopt.

ii. The Commission should revise its requirements regarding service providers, which must not include adviser/fund affiliates.

Most, if not all, advisers and funds will rely on third parties to administer at least some component of their cybersecurity program, even if only to provide certain security tools and training related to those tools. Just as an institution's overall cybersecurity program should be centered on a risk-based approach, we believe that vendor oversight should likewise be based on a principled regime. As a part of an adviser's or fund's cyber policies and procedures, an adviser/fund would be required to oversee "any service providers that receive, maintain, or process adviser or fund

---

continued assurances of the state of their defensive capabilities and underscore the fact that penetration testing can be quite costly.

[92] We observe that many requirements under NYDFS Part 500 Cybersecurity Requirements for Financial Services Companies ("NYDFS Part 500") are qualified by a risk assessment. *See, e.g.*, 23 CRR-NY 500.12(a) ("Based on its risk assessment, each covered entity shall use effective controls, which may include multi-factor authentication or risk-based authentication, to protect against unauthorized access to nonpublic information or information systems."); CRR-NY 500.15 ("As part of its cybersecurity program, based on its risk assessment, each covered entity shall implement controls, including encryption, to protect nonpublic information held or transmitted by the covered entity both in transit over external networks and at rest.").

[93] *See* CISA and FBI Alert AA22-074A, Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability (March 15, 2022), *available at* https://www.cisa.gov/uscert/ncas/alerts/aa22-074a ("As early as May 2021, Russian state-sponsored cyber actors took advantage of a misconfigured account set to default MFA protocols at a non-governmental organization (NGO), allowing them to enroll a new device for MFA and access the victim network. The actors then exploited a critical Windows Print Spooler vulnerability, 'PrintNightmare' (CVE-2021-34527) to run arbitrary code with system privileges. Russian state-sponsored cyber actors successfully exploited the vulnerability while targeting an NGO using Cisco's Duo MFA, enabling access to cloud and email accounts for document exfiltration.").

information, or are otherwise permitted to access their information systems and any information residing therein."[94] We strongly believe the Commission should narrow this set of service providers to exclude adviser/fund affiliates under common control and subject to the same enterprise cybersecurity program. To that end, all proposed cybersecurity policy and procedure requirements should apply only to certain "named service providers"—i.e. administrators or transfer agents—that are not affiliates of the institution.[95]

Specifically, proposed rules 206(4)-9 and 38a-2 require advisers and funds to ensure, through a written contact, that providers implement and maintain appropriate cybersecurity measures and practices. This proposed requirement implies the amendment of current contracts and due diligence procedures in order to incorporate the same cybersecurity requirements imposed on advisers and funds, which would be incredibly costly for firms that may have hundreds of contracts with vendors—all of which would need to be scrubbed and renegotiated, and in some circumstances, terminated.[96] The Commission should not impose a contractual obligation that indirectly imposes requirements on service providers, particularly where those providers are highly regulated banks that comply with multiple existing domestic and international cybersecurity regulations. Further, the Commission should not require advisers to terminate contracts if doing so would harm the ability to provide services to clients. The Commission should instead provide guidance and transitional provisions for advisers to enable them to continue to provide advice and investment management in the best interest of the impacted clients while seeking a suitable replacement service provider.

Alternatively, the Commission can require that appropriate due diligence programs be put in place, but the implementation of the cybersecurity program should solely be the responsibility of the service provider. We also observe that registrants subject to Regulation S-P already have strong contract provisions and oversight processes to protect customer and shareholder personal information.[97] Instead of offering a series of arbitrary oversight prescriptions, the Commission should instead, in the context of service provider agreements, provide firms—particularly smaller institutions—with suggested objectives-based language for contracts.[98]

---

[94] 87 Fed. Reg. 13531.

[95] *See id.* at 13533 (Comment Request #14); *id.* at 13526 (defining "named service providers").

[96] That, in turn, could have a deleterious effect on the vendor base, as smaller vendors would get squeezed out, which would undercut our members' desire to engage with smaller firms and diverse vendors. While we believe that all vendors should be held to a high standard of care, we caution against enacting any rules that would negatively impact small and diverse vendors.

[97] *See* 17 C.F.R. Appendix A to Subpart C of Pt. 248 VI.(c) ("Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.").

[98] At the very least, the Commission should clarify the requirements for a written contract between an adviser/fund and any service provider to address practices described in paragraphs (a)(1), (2), (3)(i), (4) and (5) of proposed rules 38a-2 and 206(4)-9. We observe that some of these practices are not applicable to service providers; for example, a service provider is not able to ensure the protection of information residing in fund information systems or detect incidents in the funds' systems.

The Commission's approach to service providers should allow for flexibility and indeed recognize that many firms, particularly small firms, have little leverage in negotiating with large service providers. Imposing strict contractual requirements could put companies in the position of choosing to either forego necessary services or to enter into contracts that do not comply with the rules. Requirements for oversight in contracts with vendors like SaaS providers and cloud-hosting providers should be limited. Meanwhile, contractual requirements for oversight of service providers that are highly regulated banks offering services such as fund accounting and administration, custody, and transfer agency, should be limited given that such entities must comply with multiple cybersecurity regulations. In those cases where specific contractual terms are not feasible or needed, a company could choose to manage the cybersecurity risk with a third party service provider in other ways, such as due diligence and ongoing assessments, through cyber risk insurance, or through other means.

iii. **Board oversight should be proportionate.**

The proposed risk management rules would require a fund's board to both initially approve a fund's cybersecurity policies and procedures, as well as annually review a written report on cybersecurity incidents and any "material changes" to such policies and procedures. Specifically, a fund must prepare an annual written report that at a minimum describes the "review, the assessment, and any control tests performed, explains their results, documents *any cybersecurity incident that occurred since the date of the last report*, and discusses any material changes to the policies and procedures since the date of the last report" (emphasis added).[99]

While we recognize the importance of firms maintaining robust governance structures and comprehensive compliance programs with a reporting line to escalate cyber issues to senior management and the board (or board committee), we believe the requirement that boards approve policies and procedures and exercise formal oversight is too prescriptive and crosses into the realm of management.

The requirement that the annual report to a fund's board "documents *any cybersecurity incident*" occurring since the last report is too broad, especially given the possible breadth of the definition of "cybersecurity incident" under the proposed rules.[100] The burdens of gathering and standardizing reporting on any cybersecurity incident from various disciplines involved in a fund's operations, such as business continuity, errors, and data confidentiality and integrity, would be substantial. We do not believe that a board would benefit from receiving reporting on less-significant cybersecurity incidents and recommend that some materiality qualifier be added to any finalized language.[101]

A fund's board should also not be required to approve the cybersecurity policies and procedures of third-party service providers. This would go beyond existing best practices with respect to third-

[99] 87 Fed. Reg. 13593.

[100] For purposes of this section, "cybersecurity incident" is currently defined as "an unauthorized occurrence on or conducted through a fund's information systems that jeopardizes the confidentiality, integrity, or availability of a fund's information systems or any fund information residing therein." *Id.* at 13589.

[101] Similarly, a materiality qualifier should be added to proposed rule 206(4)-9(b)(2) regarding the contents of an adviser's annual written. *See id.* at 13593 (describing the proposed adviser annual review and required written report).

party due diligence without providing any clear benefit in improving cybersecurity. Firms should certainly have a process to review the cybersecurity practices of their service providers and boards should review that process; however, a board should not be forced to approve and micromanage the cybersecurity policies and procedures of every separate legal entity that provides products or services to the firm. If a particular business arrangement represents an unusual risk from a cybersecurity standpoint, then it can be escalated to the board through normal channels.

The proposed rules also fail to account for the fact that many large organizations have one cybersecurity program for the entire firm; as currently drafted, the rules would require each fund to have the firm's policies and procedures reviewed by the fund's board, which is not workable for our members. Where funds are affiliates operating under an enterprise program, board oversight should take place at the parent level, not at the individual fund level.

We also observe that existing laws and regulations already require oversight of cybersecurity programs by boards. There is no evidence to show that such requirements have resulted in less rigorous board oversight or weaker cybersecurity postures than if the existing obligations were imposed on a majority of the independent directors.

We suggest that boards delegate to the adviser the requirement to maintain a cybersecurity program and receive reporting. To that end, we refer the Commission to rule 18f-4 under the Investment Company Act, which requires funds to adopt and implement a written derivatives risk management program that includes policies and procedures reasonably designed to manage the fund's derivatives risks. A fund's board, under this rule, is required to approve a derivatives risk manager responsible for administering the program. We respectfully suggest the Commission accordingly shift oversight responsibility to the fund's adviser.

Additionally, we observe that not all changes to policies and procedures warrant review and request that the Commission provide specific examples of the kinds of "material changes" that should be highlighted in a written report. Most firms already have in place policy governance programs that include an annual review and update policies to reflect changes in risks and business practices.

iv. **Certain procedures should be excluded from annual adviser and fund reviews.**

Proposed rule 206(4)-9 under the Advisers Act requires an annual review of cybersecurity policies and procedures, and proposed rule 38a-2 under the Investment Company Act similarly require that a fund's cybersecurity policies and procedures be reviewed and assessed at least annually.

We request that tactical and operational documents be excluded from the types of "procedures" that would receive a formal review. Although certain firm wide and divisional policies and standards receive regular review under a risk-based approach, "procedures" may be more tactical and operational by design, maintained at a legal entity or business unit level, and may not receive formal review by CISO-level leadership. We accordingly do not believe such procedures should be subject to an annual review under the proposed requirements.

v. The Commission should fine-tune its proposed recordkeeping requirements.

As part of the proposed risk management rules, the Commission has put forward new recordkeeping requirements for advisers and funds. The proposed rules would require advisers and funds to maintain "records documenting the occurrence of *any* cybersecurity incident, including *any* records related to *any* response and recovery from such an incident, in the last five years" (emphasis added).[102] As currently drafted, this requirement is too broad and could potentially capture less significant information, such as log data, that may not need to be subject to stringent preservation obligations. To that end, we recommend the Commission either strike the requirement given that advisers and funds must maintain records of significant cybersecurity incidents (or reports of such incidents) or insert some materiality qualifier to prevent the unnecessary documentation and maintenance of trivial matters.

* * * * * *

SIFMA and SIFMA AMG appreciate your consideration of this request. If you have questions or would like to discuss these comments further, please reach out to Melissa MacGregor at mmacgregor@sifma.org or Lindsey Keljo at lkeljo@sifma.org.

Sincerely,

Melissa MacGregor

Melissa MacGregor
Managing Director & Associate General Counsel
SIFMA

Lindsey Keljo

Lindsey Keljo
Head & Associate General Counsel
SIFMA Asset Management Group

[102] 87 Fed. Reg. 13535. This also carries through to the proposed rules at 38a-2(a)(5)(ii) and 206(4)-9(a)(5)(ii) regarding the need to maintain policies and procedures with such written documentation of any cybersecurity incident and the response to and recovery from such an incident. *See id.* at 13588, 13593.