Managed Funds Association
The Voice of the Global Alternative Investment Industry
Washington, D.C. | New York

April 11, 2022

Via Web Submission

Ms. Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549

Re: Cybersecurity Risk Management, File number S7-04-22

Dear Ms. Countryman:

Managed Funds Association[1] ("**MFA**") welcomes the opportunity to comment on the proposed rule release from the Securities and Exchange Commission (the "**Commission**"), "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies" (the "**Proposed Rules**").[2] MFA supports the Commission's objective underlying the Proposed Rules to promote cybersecurity risk management for investment advisers.

MFA is concerned, however, with the breadth of certain aspects of the Proposed Rules. For example, the Proposed Rules would require investment advisers to develop cybersecurity risk management programs to protect a wide range of "adviser information," including information that, even if exposed by a cyberattack, would be unlikely to cause actual harm to an adviser's business or its clients. The Proposed Rules also would impose on investment advisers an obligation to require a wide range of service providers to adopt their own cybersecurity risk management programs that effectively comply with the Proposed Rules, even those service providers that are not subject to Commission oversight or that do not provide critical services to

[1] MFA represents the global alternative investment industry and its investors by advocating for regulatory, tax and other public policies that foster efficient, transparent, and fair capital markets. MFA's more than 150 members collectively manage nearly $1.6 trillion across a diverse group of investment strategies. Member firms help pension plans, university endowments, charitable foundations, and other institutional investors to diversify their investments, manage risk, and generate attractive returns over time. MFA has a global presence and is active in Washington, London, Brussels, and Asia.

[2] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 13524 (Mar. 9, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-03-09/pdf/2022-03145.pdf.

the investment adviser. The Proposed Rules additionally would impose overly prescriptive reporting requirements on advisers that apply when efforts to investigate and mitigate the impact of a cybersecurity incident are still underway. We believe these requirements, when taken together, will have the unintended consequence of diverting advisers' resources from designing and implementing policies and procedures that are reasonably designed to assess, monitor, and mitigate issues that an adviser has determined to be higher risk, requiring advisers to expend limited resources in attempting to assess, monitor, and mitigate a wider range of issues that have a low likelihood of presenting material risks to advisers or investors. As a consequence, we believe that the Proposed Rules may, in certain regards, potentially increase cybersecurity risks in the industry. Moreover, the costs imposed by certain aspects of the Proposed Rules will create significant barriers to entry for new advisers, thereby limiting investor choices and potentially negatively impacting other efforts by the Commission and President Biden's administration to promote greater diversity within the asset management industry.

We suggest some specific changes to the Proposed Rules below, which we believe will help the Commission better achieve its underlying objective, without the kinds of unintended and adverse consequences noted above. We encourage the Commission to consider these comments and other potential changes to the Proposed Rules by following two basic approaches consistent with the Commission's historic practices:

(1) <u>Adopt Principles-Based Rules that Avoid Prescriptive Requirements</u>

MFA believes that the Commission should amend the Proposed Rules to remove prescriptive requirements and instead adopt a principles-based set of rules that allow advisers to appropriately tailor their cybersecurity programs based on the cybersecurity risks that the adviser reasonably determines to be most relevant in light of the nature, size and scope of the adviser's business operations. In that regard, we appreciate the Commission's recognition in the release accompanying the Proposed Rules (the "**Release**") that there is no one-size-fits-all approach to addressing cybersecurity risks.

(2) <u>Coordinate the Commission's Rules and Implementation of the Rules with Existing Rules and Standards</u>

As the Commission and its staff are aware, many advisers already have adopted and implemented robust cybersecurity risk management programs. Many advisers already are subject to existing cybersecurity requirements, including National Futures Association ("**NFA**") rules for commodity trading advisors and commodity pool operators[3] and the Federal Trade Commission's Safeguards Rule for private funds.[4] MFA continues to encourage the Commission

[3] NFA Compliance Rule 2-9.

[4] Standards for Safeguarding Customer Information, 16 CFR Part 314.

to promote coordination and harmonization among existing rules and standards and the Proposed Rules to avoid inconsistencies or unnecessary duplication of requirements for advisers.

I. Executive Summary

MFA respectfully urges the Commission to revise the Proposed Amendments consistent with the recommendations below. As discussed in more detail below, we believe the Commission should amend the Proposed Rules to:

- Narrow the definition of "adviser information," which term affects the scope of many other requirements in the Proposed Rules, in order to focus on the type of information that, if compromised in a cybersecurity attack, is reasonably likely to cause actual harm to the adviser or its clients, similar to recently adopted and more narrowly drawn rules by U.S. banking regulators.

- Provide guidance that advisers can choose to, but are not required to, utilize recognized frameworks, such as the National Institute of Standards and Technology ("**NIST**") Cybersecurity Framework ("**CSF**") for reference when developing their cybersecurity policies and procedures.

- Provide a safe harbor for investment advisers that develop their cybersecurity risk management programs based on the CSF or based on National Futures Association requirements for firms that are regulated by the Commodity Futures Trading Commission.

- Focus on service providers that provide critical services, permit investment advisers to rely on service providers that have a cybersecurity risk management program that applies one of several criteria discussed below, and reflect the commercial reality that investment advisers often will not have the ability to require service providers to amend their contracts or practices as required by the Proposed Rules.

- Narrow the scope of the incident response and recovery requirements in the Proposed Rules to apply only when there is a data breach that leads to actual harm.

- Remove or clarify language in the Release that indicates the Proposed Rules would require investment advisers to adopt cybersecurity risk management programs that go beyond existing practices and standards.

- Clarify that the Proposed Rules do not require one specific approach for investment advisers to address recoverability from significant operational disruption.

- Narrow the scope of adviser policies and procedures designed to satisfy the threat and vulnerability management element to allow investment advisers to focus on addressing those threats and vulnerabilities that the adviser has determined pose meaningful risk of substantial, actual harm to clients or the adviser's business.

- Define standards with respect to the Commission's expectations regarding multi-factor authentication.

- Simplify the proposed reporting rule to: (1) provide investment advisers with more flexibility regarding the timing of submitting a notice to the Commission; (2) eliminate the detailed initial reporting requirements to require only a notification to the Commission, similar to recently adopted requirements by U.S. banking regulators, and (3) eliminate the requirement to amend an initial notification report.

- Provide a thirty-day timeline for investment advisers to disclose significant cybersecurity incidents to investors, to begin upon resolution of the significant cybersecurity incident.

- Supplement the Proposed Rule to require investment adviser cybersecurity risk management programs to include: (1) training of employees; (2) testing of systems; and (3) monitoring of suspicious activities.

II. Introduction

As stated above, MFA and its members support the Commission's objective of promoting robust cybersecurity risk management, an obligation that our members already devote significant time and resources to address. In considering how best to promote cybersecurity risk management, it is critical that any final rules provide investment advisers with sufficient flexibility to take into account the differences between asset management firms and other types of financial institutions (such as banks) and the differences among asset management firms, including with respect to their resources and likely risks. A principles-based approach that provides flexibility will help ensure that advisers can design cybersecurity risk management programs that are well suited to the risks they have identified and to use service providers and risk management tools that they believe are best suited to meet the adviser's needs.

As noted above, we appreciate the Commission's recognition in the Release that there is not a one-size-fits-all approach to addressing cybersecurity risks; however, we believe that certain provisions in the Proposed Rules, particularly those related to the scope of "adviser information" that is subject to the Proposed Rules, requirements related to service providers, and the reporting of cybersecurity incidents, would create prescriptive requirements that are not well suited to the diverse asset management industry.

We are concerned that overly prescriptive requirements, or rules that would require advisers to devote resources to address low-likelihood events or address risks that are unlikely to result in actual harm to the adviser's business or clients, could have the unintended consequence of increasing cybersecurity risks across the system, contrary to the Commission's objectives. In that regard, we believe that the proposed amendments discussed below will better achieve the

Commission's stated objectives in issuing the Proposed Rules and will avoid some of the unintended consequences that we believe could result from the Proposed Rules.

III. Recommended Amendments

A. Proposed Cybersecurity Risk Management Rule

Proposed Rule 206(4)-9 would require investment advisers that are registered or required to be registered under the Advisers Act to adopt written policies and procedures that include: (1) a risk assessment; (2) controls related to user security and access; (3) information protection; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident and response.[5] MFA generally agrees that an investment adviser's cybersecurity risk management program should address each of these elements, but we have concerns regarding certain aspects that are included within Proposed Rule 206(4)-9.

MFA also agrees with the Commission that "given the number and varying characteristics (*e.g.*, size, business, and sophistication) of advisers, . . . [such advisers] need the ability to tailor their cybersecurity policies and procedures based on their individual facts and circumstances."[6] The cybersecurity risks relevant to an investment adviser differ from the risks relevant to other types of financial services firms (such as banks, broker-dealers, or insurance companies) and will also differ among advisers based on the nature and scope of their operations, size, and clients.

Investment advisers need flexibility to tailor their cybersecurity policies to be able to prioritize their resources on the risks they have identified. Cybersecurity risk management programs that are appropriately tailored to an adviser's business and material risks will create more effective cybersecurity programs and better protect the interests of investors. We also agree with the Commission that "cybersecurity threats are constantly evolving, . . . [so] this approach would allow an adviser's . . . cybersecurity policies and procedures to evolve accordingly as firms reassess their cybersecurity risks."[7]

i. The Commission should narrow the definition of "adviser information"

As discussed further below, the scope of the defined term "adviser information" significantly affects the majority of requirements established by the Proposed Rules. As the Commission is aware, each of the five elements of Proposed Rules 206(4)-9(a) relates to adviser information and adviser information systems. Although we address other concerns related to

[5] Rule citations in this letter are to rules proposed or adopted under the Investment Advisers Act of 1940, unless stated otherwise.

[6] *See* Release, *supra* note 2, at 13528.

[7] *Id*. at 13528.

specific aspects of the Proposed Rules below, we believe that a more appropriately tailored definition of "adviser information" is required for the Proposed Rules to achieve an appropriate scope. We further believe that a more narrowly tailored definition of "adviser information" may make it easier for the Commission to address many of the issues discussed in more detail below.

The Proposed Rule defines "adviser information" extremely broadly to mean "any electronic information related to the adviser's business, including personal information, received, maintained, created, or processed by the adviser."[8] The term "personal information," in turn, means: "(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."

Read together, the proposed definition of "adviser information" could pick up any information system or service provider that has access to personal information, regardless of whether that information is reasonably likely to create actual harm to the adviser's business or to its clients. For example, read literally, the proposed definitions could cause a vendor that plans a social event for an adviser to be caught in scope because the vendor has the names of adviser employees. Other service providers, such as car service providers, may similarly have access to certain information that falls within the broad definition of "personal information" but do not have the type of information that could cause actual harm to the adviser or its clients, if the service provider were the target of a cybersecurity breach.

Accordingly, we encourage the Commission to amend the definition of "adviser information" to mean "any electronic information, including personal information, received, maintained, created, or processed by the adviser, the compromise of which would create or would be reasonably likely to create actual harm to the adviser or its clients." We note that tying the definition of "adviser information" (and by reference the definition of "cybersecurity "incident") to information that causes actual harm is consistent with recently adopted rules from the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Company (the "**Computer-Security Incident Rules**").[9] In response to public comments that including potential harms within the definition of "computer-security incident" was too broad, the final Computer-Security Incident Rules narrowed the term to mean "an occurrence that results in actual harm to the confidentiality,

[8] *See* Release, *supra* note 2, at 13529.

[9] *See,* Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, (November 23, 2021), available at: https://www.govinfo.gov/content/pkg/FR-2021-11-23/pdf/2021-25510.pdf.

integrity, or availability of an information system or the information that the system processes, stores, or transmits."[10] We believe that amending the definition of "adviser information" in a similar manner will better align the rules with the types of adviser data likely to cause material harm if it were to be compromised in a cybersecurity incident. Absent a refined definition of "adviser information," we believe that it will be difficult, if not impossible, for an adviser to be able to adequately tailor its cybersecurity risk management program based on the adviser's business and identified risks.

ii. The Commission should provide guidance that advisers can choose to, but are not required to, utilize recognized frameworks for reference when developing their cybersecurity policies and procedures

As stated above, MFA supports a principles-based approach to the Proposed Cybersecurity Risk Management Rule, which we believe is necessary to provide advisers with appropriate flexibility in designing and implementing their policies and procedures. In certain respects, the Release suggests that the Commission intended to propose a principles-based framework. We encourage the Commission to clearly state that the Proposed Rules are intended to be, and will be interpreted by the Commission to be, principles-based. In adopting principles-based rules, it would be helpful for the Commission to provide guidance that advisers can choose to use as a resource when implementing those rules.

The Release, however, does not provide sufficient guidance or clarity to advisers, leaving significant uncertainty for advisers as to the Commission's expectations for advisers in connection with an adviser conducting a risk assessment. There are a variety of existing standards and guidance, with varying levels of granularity and scope, some of which would provide helpful clarity to advisers, though we note that some standards (for example, standards intended to be used by larger, more complex financial institutions like banks) are likely to be overly complex and burdensome in light of the risk profile of many advisory businesses.

While we do not believe the Cybersecurity Risk Management Rule should specify a particular standard, we believe it would be helpful for the Commission to provide guidance that advisers can choose to, but are not required to, utilize recognized frameworks for reference when developing their cybersecurity policies and procedures.

For example, we believe frameworks such as the National Institute of Standards and Technology ("**NIST**") Cybersecurity Framework ("**CSF**") would be a valuable reference for advisers regarding accepted practices in conducting their risk assessment and developing policies and procedures based on the adviser's risk assessment. We believe that the ability of organizations to adopt varying degrees of maturity across the CSF and determine which

[10] *Id.* at 66442.

particular controls the organization should adopt based on the organization's risks make the CSF a useful reference point, while preserving a principles-based approach to the rules.

While we believe that the NIST CSF would provide a useful reference point for advisers that want to use it as such, we also believe that any such guidance from the Commission should make clear that an investment adviser can choose to refer or not refer to those frameworks and standards as it deems appropriate in developing its cybersecurity risk management program. We further encourage the Commission to provide similar guidance that advisers can choose to, but are not required to, refer to existing Commission guidance and audit priorities, including the Cybersecurity Profile from the Financial Services Sector Coordinating Council, [11] or the cybersecurity related NFA compliance rules and the NFA's interpretive notice relating to those rules as resources. Of course, consistent with a principles-based approach to the rules, investment advisers should be permitted to refer to other frameworks and standards to the extent an adviser believes those standards are more appropriate to its particular business and risks.

Providing references to existing frameworks and standards in the form of guidance, rather than as part of the rule itself, can help to preserve the flexibility that advisers need to tailor their risk assessments and policies and procedures, while providing useful guideposts that can help provide clarity to advisers and promote strong industry practices. In referencing the CSF, the Commission should clearly state that advisers can build their cybersecurity risk management programs to address the areas that they determine to be of greatest risk and are not required to do the same detailed assessment of areas that they do not believe present likely risks (*i.e.*, an adviser may remove from the assessment scope elements of the referenced controls in the CSF that are not relevant to the adviser's business or which do not present material risk). We believe that confirming that advisers have the flexibility to conduct risk assessments that focus on those areas they have determined to be of importance will avoid the adviser having to dilute its resources to assess areas it does not believe to be of relevance or importance in terms of risk.

iii. <u>The Commission should provide a safe harbor for investment advisers that develop their cybersecurity risk management programs based on the CSF or based on NFA requirements for CFTC-regulated firms</u>

Although we believe the Commission should provide guidance that the CSF can be used as a reference for advisers rather than a requirement, we also encourage the Commission to consider providing a safe harbor that would deem an investment adviser whose policies and procedures are developed in accordance with existing guidelines from NIST to be in compliance with Rule 206(4)-9. We also encourage the Commission to provide a safe harbor for investment advisers that are regulated by the Commodity Futures Trading Commission ("**CFTC**") and that

[11] The Cybersecurity Risk Profile is available at: https://cyberriskinstitute.org/the-profile/.

comply with the cybersecurity related NFA compliance rules and the NFA's interpretive notice relating to those rules.[12]

We note in this regard that Regulation Systems and Compliance and Integrity provides an explicit safe harbor from liability[13] and also provides an effective safe harbor that deems policies and procedures that are consistent with current SCI industry standards to be reasonably designed for purposes of the regulation.[14] We note that several states also provide safe harbors that refer to the NIST CSF (such as those in Ohio and Connecticut).

Providing a compliance safe harbor will provide certainty to advisers making good faith efforts to comply with any final Cybersecurity Risk Management Rule, while minimizing the risk of hindsight judgment by Commission staff in the absence of clear standards. In addition, the specialized nature of cybersecurity expertise and limited availability of existing resources in the cybersecurity industry will create challenges for many advisers to obtain services and likely will impose significant costs on advisers. Providing a safe harbor based on existing and well understood standards can provide a more efficient and potentially cost-effective framework for advisers working to comply with any final rule. A safe harbor based on the CSF also will help the Commission accomplish its objective underlying the Proposed Rules by providing an incentive for advisers to adopt programs that are based on existing industry practices that have been recognized as effective by other financial regulators.

iv. Amend the Proposed Rules with respect to service providers

The Proposed Cybersecurity Risk Management Rule would impose significant requirements on advisers to manage numerous service providers that provide a wide range of services. As drafted, the Proposed Rule would require advisers to have contracts with a large number of service providers that include contractual provisions based on the Proposed Rule, even if the service provider is not subject to Commission jurisdiction. The scope of service providers covered by the Proposed Rule is overly broad because it includes any service provider that receives, maintains, or processes adviser information, which, as discussed above, is defined too broadly. In addition, the Proposed Rule is not limited to service providers that provide critical services to an investment adviser. Together, the broad scope of service providers covered by the Proposed Rule is concerning because those service providers that are not subject to

[12] *See* NFA Interpretive Notice 9070 – NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs, available at: https://www.nfa futures.org/rulebook/rules.aspx?RuleID=9070&Section=9#:~:text=NFA%20Compliance%20Rule%202%2D9%20places%20a%20continuing%20responsibility%20on,of%20their%20commodity%20interest%20activities.

[13] 17 CFR § 242.1001(b)(4).

[14] 17 CFR § 242.1001(a)(4).

Commission oversight may be unwilling to agree to be governed by standards set by a regulator that does not regulate them. Many advisers have been pushing unsuccessfully for these terms with vendors for years and, because investment advisers are a relatively small part of the customer base for many service providers, it is unlikely that adoption of the Proposed Rules will change that outcome. Further, in the interest of their own security, some service providers may be unwilling to agree to provide advisers as a contractual requirement the type of information contemplated by the Proposed Cybersecurity Risk Management Rule. Accordingly, the provisions of the Proposed Rules related to the cybersecurity risk management of service providers needs to be principles-based so that implementation of the Proposed Rules can be tailored appropriately to the risks presented by a particular service provider and to commercial realities related to an adviser's ability to require service providers to make changes to their cybersecurity risk management programs.

Advisers should, and already do, conduct reasonable due diligence when selecting critical service providers and engage in ongoing monitoring of those service providers. A reasonable diligence and oversight approach can improve cybersecurity by allowing advisers to work with service providers they believe have strong compliance programs, even if those programs are not fully aligned with Commission rules that do not apply to the service provider. Under the Proposed Rule, advisers may be unable to contract with service providers that the adviser believes have exemplary security practices to the extent those practices do not fully align with the Proposed Rules, or if the service provider does not agree to certain contractual provisions. Likewise, advisers may not be able to use what it believes are exceptional security tools offered by such providers in ways that the adviser believes enhance the security of its systems, but which do not fully align with the Proposed Rules. In each of these circumstances, advisers could be forced to transition to alternative arrangements that may be less protective or, to the extent advisers are forced to transition to more in-house services, potentially result in the concentration of the adviser's cybersecurity risks.

Moreover, the Proposed Rules should not require advisers to impose requirements on service providers, particularly because in many cases advisers will be unable to do so. For example, advisers are unlikely, as a commercial matter, to be able to force companies like Microsoft or Amazon Web Services to make material changes to those companies' terms of service. Advisers also are unlikely to be able to force banks, broker-dealers, or self-regulatory organizations to agree to cybersecurity requirements that differ from the cybersecurity programs those institutions already have developed in order to comply with their own regulatory and internal risk management requirements.

To address these concerns, we encourage the Commission to amend the aspects of the Proposed Rules addressing service providers to focus on critical service providers, rather than all service providers that receive, maintain, process, or otherwise access "adviser information,"

which, as discussed above, is an expansive term, which does not target the subset of information that presents meaningful risk to the adviser or its clients. In that regard, we also encourage the Commission to confirm that advisers can use reasonable judgment to determine which of their service providers they believe to be critical. Focusing any final rule on critical service providers also will better allow an adviser to allocate its resources to those areas that the adviser has determined pose the most significant risks to its business.

Finally, the Commission should amend the Proposed Rule to explicitly permit advisers to rely on service providers that have a cybersecurity risk management program that meets one of the following criteria: (1) it complies with federal or equivalent international regulatory requirements applicable to the service provider (such as rules issued by the Commission, the Board of Governors of the Federal Reserve System, or the CFTC); (2) it is authorized at the Moderate or High impact levels under the Federal Risk and Authorization Management Program ("**FedRAMP**"); or (3) it has been audited by a third party based on existing industry standards (such as ISO 27000, NIST 800-53 or SOC2).

v. The Commission should amend the incident response and recovery requirements[15] in the Proposed Cybersecurity Risk Management Rule to apply when there is data loss that leads to actual harm

Advisers design business continuity and disaster recovery policies, procedures and technical solutions based on their assessment of risks that are most likely to cause actual harm and that they are most likely to actually face, rather than attempting to address all hypothetical or theoretical risks that may arise. In order to better achieve the goals of the Proposed Rules, the Commission should clearly articulate that advisers can use reasonable judgment in determining the risks they are likely to face, establishing recovery time objectives and recovery point objectives that advisers determine are appropriate to their business, and use reasonable judgement in determining, designing, and tailoring their policies and procedures accordingly. In the absence of such a clarification, advisers would face significant hindsight risk of being deemed not to have sufficient policies only after an actual, even if unanticipated, cybersecurity event, and despite an adviser's good faith efforts in designing its policies and procedures. This risk is heightened because the incident response and recovery requirements incorporate the broad definition of adviser information indirectly through the use of the term "cybersecurity incident" and also directly by requiring policies and procedures that are reasonably designed to protect adviser information systems and adviser information.

To address these concerns, we encourage the Commission to narrow the definition of "cybersecurity incident" to mean an unauthorized occurrence that creates, or is reasonably likely to create, actual harm, not merely one that "jeopardizes the confidentiality, integrity, or

[15] *See* Release, *supra* note 2, at 13532-33.

availability of an adviser's information systems or any adviser information residing therein."[16] The proposed definition, particularly in combination with the broad definition of "adviser information," could lead to virtually any unauthorized occurrence triggering the Proposed Rule's requirements related to cybersecurity incidents, even when there is no actual harm to clients or actual and material disruption to an adviser's business. Focusing the definition on incidents that produce actual harm will avoid overly burdensome obligations on advisers, while ensuring the rule still captures meaningful incidents within its scope.

vi. The Commission should remove or clarify language that goes beyond existing practices and standards

The Proposed Rules and the Release contain language that could indicate the Commission expects advisers to design and implement cybersecurity risk management programs that go beyond existing standards. This concern is compounded by the broad definition of "adviser information" (discussed above) which, if not amended, would significantly expand the scope of an adviser's systems that need to be addressed by the adviser's cybersecurity risk management program.

For example, the Proposed Rules would require an adviser to describe how the adviser assesses and prioritizes its cybersecurity risks. We agree that advisers need to assess and prioritize the risks that they believe are most relevant to their business. We encourage the Commission to confirm that this obligation is not intended to require advisers to quantify their cybersecurity risks. A requirement or expectation that advisers quantify their cybersecurity risks goes beyond established standards applicable to other financial institutions and the federal government, and it would require advisers to devote substantial resources that would be more effectively allocated elsewhere.

As another example, the Proposed Rule requires advisers to categorize risks based on an inventory of the components of their information systems, which goes well beyond the CSF and other industry standards, including the standards set forth in NIST 800-53.[17] Assessment of network risks, as opposed to component risks, is a well-understood cybersecurity activity. We believe that requiring advisers assess risks at a component level of their information systems will divert resources better used to assess key risks and is unnecessary, as demonstrated by the scope of current industry standards used by large financial institutions and the federal government.

To the extent the Commission intends the Proposed Rules to require cybersecurity risk management programs that do go beyond existing requirements, guidance, and standards, it

[16] Proposed Rule 206(4)-9(c).

[17] Security and Privacy Controls for Information Systems and Organizations, available at: https://csrc nist.gov/publications/detail/sp/800-53/rev-5/final.

should clearly identify those expectations. Before adopting any such requirements, however, the Commission should provide an opportunity for public review and comment of those proposals.

vii. The Commission should clarify that the Proposed Cybersecurity Risk Management Rule does not require one specific approach for investment advisers to address recoverability from significant operational disruption

The Release suggests that advisers should consider risks associated with having services "concentrated"[18] at a particular service provider, such as a cloud service provider or a service provider that helps calculate an investment fund's net asset value. In discussing those risks, the Release suggests that an adviser should consider identifying "alternative processes or vendors" to perform the services.[19] We appreciate that the Proposed Rules do not on their face require investment advisers to use redundant services or service providers to reduce the risk of operational disruption from a cybersecurity incident. We encourage the Commission to confirm that the language in the Release is not intended to suggest that an investment adviser must use redundant services in addressing risks of operational disruption.

While the use of redundant services in some situations may reduce the risk of certain operational disruptions, as reflected today in certain industry practices, such redundancy is both expensive and complicated to implement (perhaps prohibitively so for smaller firms) as the infrastructure utilized in conjunction with different service providers are not necessarily interchangeable. In other situations, adding redundant service providers may in fact increase the risk of other operational disruptions and information compromise (if, for example, data integrity becomes compromised if the data at different service providers were to become out of sync) by spreading firms' information through additional systems, exposing that information to additional attack vectors.

We encourage the Commission to clarify that the commentary in the Release that is noted above is intended to mean that advisers should take concentration risks into consideration as part of their risk assessments and, if the nature of the services provided by the service provider is critical to their business, that adviser should address risks of prolonged disruptions due to a cybersecurity incident. This clarification would better focus on the need for advisers to address the ability to recover from critical disruptions to its services, rather than suggesting that one potential method of recoverability is expected or required. In that regard, we believe it would be helpful for the Commission to state that advisers can address risks of critical service disruptions in different ways, including the use of redundant services, having the ability to recover services

[18] *See* Release, *supra* note 2, at 13530.

[19] *Id.*

within an acceptable period of time, replacement of the service provider, assessment of a critical service provider's business continuity protocols, and as appropriate, manual processing.

viii. The Commission should narrow the scope of adviser policies and procedures designed to satisfy the threat and vulnerability management element

The Proposed Cybersecurity Risk Management Rule requires firms to "detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to adviser information systems and the adviser information residing therein."[20] The proposed requirement, as drafted, is overly broad and could result in advisers having to allocate resources to cover all potential cybersecurity threats and vulnerabilities, even low-risk vulnerabilities that are unlikely to occur and/or unlikely to cause material harm even if they were to occur. MFA believes that this requirement should be narrowed to permit advisers to adopt measures that are reasonably designed to address those threats and vulnerabilities that the adviser has determined pose meaningful risk of substantial, actual harm to clients or the adviser's business, including by amending the scope of the Proposed Rule to apply to a more narrowly tailored definition of "adviser information," as discussed above. Rules that would require advisers to implement cybersecurity risk management programs that prioritize breadth over depth in their cybersecurity risk assessments are likely to be less effective than rules that permit advisers to focus their resources on areas they reasonably believe present the greatest risk to clients or the adviser's business. Patch management is another example of where Rules that are over-proscriptive may lead to increased cybersecurity risk. Patch's must be tested, and certain patches may be reasonably delayed or skipped altogether. Advisers should be allowed to determine an appropriate patch management policies and procedures that address the adviser's assessment of risk.

ix. The Commission should define standards with respect to the expectations of multi-factor authentication in the proposed information protection element

The Proposed Cybersecurity Risk Management Rule requires advisers to adopt "controls designed to minimize user-related risks and prevent unauthorized access to adviser information systems and adviser information residing therein."[21] In discussing this requirement, the Release discusses multi-factor authentication as one component of a control system.[22] Neither the Release nor the Proposed Rules define multi-factor authentication, which is a general term that has various commonly-held definitions. Multi-factor authentication is likely to be an important component of an adviser's user security and access controls and, accordingly, the Commission

[20] Proposed Rule 206(4)-9(a)(4).

[21] Proposed Rule 206(4)-9(a)(2).

[22] *See* Release, *supra* note 2, at 13531-13532.

should provide clarification regarding that term. For example, we encourage the Commission to provide guidance that an adviser could take into account any or all of the following circumstances in determining an appropriate multi-factor authentication protocol: (1) accessing a vendor network or portal that does not require multifactor authentication; (2) accessing a password-protected internal network from within a company office secured by keycards or other circumstances in which such single-factor authentication must originate from the corporate network; or (3) a customer accessing an adviser-created portal that does not contain nonpublic personal information and does not provide access to the internal adviser network. Advisers also should have the ability to determine appropriate reasonably equivalent compensating or mitigating controls that may be implemented instead of multi-factor authentication, similar to what is permitted by the New York Department of Financial Services.[23]

Further, the Commission should confirm that advisers, when developing access controls and restrictions, are permitted to determine what type of access restrictions are appropriate, factoring in the impact on clients and investors that restricting employee access can have. As with other requirements of the Proposed Rules, the scope of the Proposed Rule regarding information protection is extremely broad because of the references to the broad definition of "adviser information." Accordingly, in the absence of such clarification, advisers may be incentivized to adopt overly conservative approaches in developing access restrictions, which could negatively affect clients and investors by impairing the adviser's ability to function efficiently.

B. Proposed Reporting Rule

Proposed Rule 204-6 would require an investment adviser that is registered or required to be registered under the Advisers Act to report any significant cybersecurity incident or significant fund cybersecurity incident to the Commission on Form ADV-C and to promptly amend any previously filed Form ADV-C if there are material inaccuracies in a previously filed Form or material new information to include on a previously filed Form. MFA believes that the Commission should adopt a more flexible reporting deadline (*e.g.*, promptly after a cybersecurity incident), similar to NFA requirements.[24] Providing for a flexible reporting deadline will permit an adviser that is in the midst of a cybersecurity incident to devote its resources to addressing and mitigating such incident rather than having to reallocate resources to prepare a report for the Commission within an expedited timeframe. For many advisers, the persons with responsibility for identifying, mitigating, and responding to a cybersecurity incident also would be involved in assisting the preparation of the report to the Commission. As such, Commission reporting,

[23] *See* Guidance on Multi-Factor Authentication (Dec 7, 2021), available at: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211207_mfa_guidance.

[24] *See* NFA Interpretive Notice 9070 – NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs, *supra* note 14.

particularly detailed reports and reporting requirements triggered by a wide range of cybersecurity incidents, are likely to interfere with an adviser's efforts to mitigate the effects of a cybersecurity incident.

If the Commission determines a specific deadline is appropriate, MFA encourages the Commission to extend the proposed 48 hour deadline. Many regulatory agencies and jurisdictions require 72 hours for such reports (the main time period used by the New York Department of Financial Services, the European Union relating to the General Data Protection Regulation, and other jurisdictions, for example). Similarly, President Biden recently signed into law the Cyber Incident Reporting for Critical Infrastructure Act, which requires a 72-hour "cyber incident notification,"[25] and the Commission just proposed a reporting timeline of "four business days" for public reporting companies to report a cybersecurity incident to the Commission.[26] While even these deadlines likely would not address all of the concerns discussed above, these deadlines would be preferable to the Commission's proposed 48-hour deadline.

To the extent that the Commission determines to include a specific reporting deadline, we also encourage the Commission to require advisers submit less detailed information in their initial reports. Permitting advisers to submit less detailed initial reports will better ensure the Commission receives timely notice of cybersecurity incidents while minimizing the risk that advisers and their personnel are distracted from dealing with an incident before its impact spreads. The Computer-Security Incident Rules, for example, simply require banking organizations to notify the appropriate regulator about a notification incident (as defined in those Rules) through email, telephone or other similar methods.[27] The Computer-Security Incident Rules do not create or otherwise require banking organizations to provide specific or detailed initial reports, nor do they create specific amendment requirements. Instead, the Computer-Security Incident Rules appropriately require regulated entities to provide notice to their regulator, while avoiding the unnecessary and potentially harmful distraction that detailed notification and amendment requirements can have. We encourage the Commission to amend the Proposed Reporting Rule to require a simple notification similar to that required in the Computer-Security Incident Rules and to delete the proposed requirement to amend such initial notice.

The Commission also should coordinate its incident reporting requirement with similar requirements imposed by other regulators to avoid unnecessarily requiring advisers to have multiple reporting obligations that could further distract them from dealing with an incident and

[25] Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 117th Cong. (2022).

[26] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Securities Exchange Act of 1934 Release no. 94382 (Mar. 9, 2022), available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

[27] Computer-Security Incident Rules, *supra* note 9, at 66442.

seeking to minimize the potential impact of an incident. In that regard, the Commission should consider whether an investment adviser required to submit a notification regarding a cybersecurity incident to another federal regulator should be permitted to simply notify the Commission of that fact, which would enable the Commission to coordinate with the other regulator.

Finally, we note that the Proposed Reporting Rule requires an initial report when an adviser has a "reasonable basis to conclude" that a significant cybersecurity incident or a significant fund cybersecurity incident had occurred or is occurring. The requirement to amend a prior report does not include similar language. To the extent that the Commission does not amend the requirement to amend prior reports, the Commission should amend the Proposed Rule to include the "reasonable basis" standard for amended reports as well as initial reports.

C. Proposed Disclosure Rule

Proposed Rule 204-3(b) would require an investment adviser to deliver an amended brochure, brochure supplement, or information statement to each client promptly after the adviser amends its brochure or brochure supplement, as applicable, and the amendment includes disclosure of a significant cybersecurity incident, or materially revises information already disclosed about such an incident. For similar reasons underscoring our suggested changes to the Proposed Reporting Rule, MFA believes that the Commission should provide a thirty-day timeline for investment advisers to disclose significant cybersecurity incidents to investors, to begin upon resolution of the significant cybersecurity incident. In addition, if an adviser were required to make premature disclosures to investors while the adviser is simultaneously attempting to determine the scope of an incident and its potential impact, there is a significant likelihood of the initial disclosure being judged in hindsight to be inaccurate or incomplete. This potentially could create liability risk for adviser. Further, given the lack of certainty that often accompanies cybersecurity incidents, especially during the initial detection and mitigation stage, premature disclosure is more likely to provide incomplete or confusing information to investors than requiring disclosure within a reasonable time period after the cybersecurity incident has been resolved.

D. Additional Considerations

Finally, we note that the Release discusses additional procedures that advisers should consider but are not included in the scope of the Proposed Rules. We believe that there are additional measures that would further the objectives of the Proposed Rules without imposing undue burdens on investment advisers. Accordingly, we encourage the Commission to include in any final rule a requirement for an adviser's policies and procedures to provide for: (1) training of employees; (2) testing of systems; and (3) monitoring of suspicious activities. Many advisers

already incorporate these elements into their policies and procedures and we believe they would strengthen any final rules adopted by the Commission.

* * *

IV. Conclusion

MFA appreciates the opportunity to provide comments to the Commission on the Proposed Rules. We welcome the opportunity to discuss our views with you in greater detail. Please do not hesitate to contact Matthew Daigler, Vice President & Senior Counsel, or the undersigned, at [redacted], with any questions that you, your respective staffs, or the Commission staff might have regarding this letter.

Respectfully submitted,

/s/ Jennifer W. Han

Jennifer W. Han
Executive Vice President
Chief Counsel & Head of Global Regulatory Affairs

cc: The Hon. Gary Gensler, SEC Chairman
The Hon. Hester M. Peirce, SEC Commissioner
The Hon. Allison Herren Lee, SEC Commissioner
The Hon. Caroline A. Crenshaw, SEC Commissioner
Mr. William Birdthistle, Director, Division of Investment Management