INVESTMENT ADVISER ASSOCIATION

June 5, 2023

Via Electronic Filing

Ms. Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information; 88 Fed. Reg. 20616 (RIN: 3235-AN26)

Dear Ms. Countryman:

The Investment Adviser Association (**IAA**)[1] appreciates the opportunity to comment on the Commission's proposed new rule and related disclosure and recordkeeping amendments under Regulation S-P.[2] The Proposal would require SEC-registered investment advisers to adopt written policies and procedures for incident response programs to address unauthorized access to client non-public personal information (**PII**) and for providing timely breach notification to individuals affected by an incident involving sensitive information.

As information security threats continue to increase in prevalence and sophistication, investment advisers remain committed to protecting their clients and their businesses. Since the adoption of Regulation S-P in 2000, advisers have focused on meeting their obligation to develop and maintain policies and procedures to safeguard client information in ways that are tailored to their firms and the risks of inadvertent disclosure particular to their business operations.[3]

---

[1] The IAA is the leading organization dedicated to advancing the interests of investment advisers. For more than 85 years, the IAA has been advocating for investment advisers before Congress and U.S. and global regulators, promoting best practices and providing education and resources to empower investment advisers to effectively serve their clients, the capital markets, and the U.S. economy. Our members range from global asset managers to the medium- and small-sized firms that make up the core of our industry. Together, the IAA's members manage more than $35 trillion in assets for a wide variety of clients, including individuals, trusts, investment companies, private funds, pension plans, state and local governments, endowments, foundations, and corporations. For more information, please visit www.investmentadviser.org.

[2] *Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information*, 88 Fed. Reg. 20616 (Apr. 6, 2023), available at https://www.govinfo.gov/content/pkg/FR-2023-04-06/pdf/2023-05774.pdf (**Proposal**). The IAA is only commenting in this letter on the Proposal as it relates to investment advisers.

[3] Underscoring its strength and flexibility to address a wide range of situations, the Commission has also construed the Compliance Rule (Rule 206(4)-7) to include policies and procedures to safeguard client records and information

The IAA remains committed to supporting efforts by the Commission to protect investors, other market participants, and the financial markets more broadly from the dangers presented by information security threats. We strongly support advisers being required to maintain the confidentiality of clients' PII and to notify clients when their PII has been compromised. We have long supported a uniform preemptive data breach notification regime across regulators, to create consistency and reduce complexity.[4] Advisers currently face a burdensome, complex maze of federal and state requirements relating to the reporting of data breaches that is difficult to navigate, and we continue to urge the Commission to work with other regulators towards a uniform approach.

In the meantime, however, we understand and share the Commission's concerns and thus support the Proposal, subject to certain recommendations that we believe would further the Commission's objectives while more effectively protecting investors and streamlining unnecessary operational and compliance burdens on advisers.[5]

I. Executive Summary

We offer both general and specific comments and recommendations to improve the Proposal. Our recommendations relate to: (A) Customer Information; (B) Incident Response Program; (C) Customer Notification; (D) Recordkeeping; (E) Cost-Benefit Analysis; (F) Proposed Compliance Date; (G) Holistically Addressing Rulemakings; and (H) Coordination with Other Federal Regulators.

A. Customer Information

We support the Commission's adoption of a rule that mandates advisers to establish written policies and procedures that address safeguards for client PII, including administrative, technical, and physical measures. To more effectively target compliance efforts and resources to risk, we recommend that certain of the proposed safeguards, including the incident response program and requirements related to "Service Providers," should cover "Sensitive Customer Information," and not "Customer Information" more broadly.[6]

---

under Regulation S-P. *Compliance Programs of Investment Companies and Investment Advisers*, 68 Fed. Reg. 74714, 74716, n. 21 and accompanying text (Dec. 24, 2003) ("an adviser's policies and procedures, at a minimum, should address … [s]afeguards for the privacy protection of client records and information.")

[4] *See* Letter from IAA President & CEO Karen Barr to SEC Chair Gary Gensler, *Regulation of Investment Advisers* (May 17, 2021), available at https://investmentadviser.org/resources/regulation-of-investment-advisers/. The Gramm-Leach-Bliley Act (**GLBA**) preempts state laws only to the extent that compliance with a state law would be "inconsistent with" the requirements of the GLBA. A state law is not considered inconsistent if it provides a person with protection that is greater than the protection provided under the GLBA.

[5] We appreciate that the Commission has reopened its cybersecurity proposal for advisers. The IAA is submitting a separate comment letter on the reopened proposal.

[6] As used in this letter, capitalized terms are either defined or proposed to be defined under Regulation S-P. We describe and discuss several of these definitions below in Section II(A).

B. Incident Response Program

We support the Commission's adoption of a rule that would require advisers to adopt an incident response program to address unauthorized use of or access to client PII by implementing a program that would be "reasonably designed to detect, respond to, and recover from both unauthorized access to and unauthorized use of" this information,[7] subject to certain recommended modifications. Specifically, we recommend that the Commission:

- Limit the scope of the incident response program to protecting against unauthorized use of or access to Sensitive Customer Information, rather than Customer Information more broadly, as proposed.

- Continue to allow advisers to use a principles- and risk-based approach to tailor their assessment and containment-and-control policies and procedures.

- Narrow and clarify the definition of Service Provider to:

    - Include only those service providers that may receive, maintain, or process Sensitive Customer Information, or be permitted to access an adviser's Customer Information Systems;

    - Exclude affiliated service providers operating under a shared services or similar model; and

    - Exclude service providers that are subject to the GLBA and in a direct contractual relationship with the client.

- Recognize the tremendous challenges advisers face in negotiating written contracts with Service Providers and not require advisers to enter into written agreements with Service Providers. Instead, as we have urged in other contexts,[8] advisers should be given the flexibility to oversee their Service Providers based on the nature and size of their businesses and in light of the risks posed by the facts and circumstances.

C. Customer Notification

We support the Commission's adoption of a rule that would require advisers to provide a clear and conspicuous notice to each "Affected Individual" whose Sensitive Customer Information was, or is reasonably likely to have been, accessed or used without authorization, subject to certain recommended modifications to make the notice requirements more effective. Specifically, we recommend that the Commission modify and clarify:

---

[7] Proposal, 88 Fed. Reg. at 20680. We are asking the Commission to add "sensitive" to the definition as we discuss in Section II(B)(2) below.

[8] We discuss other relevant IAA comments below.

- The notification obligation trigger;
- The scope of Affected Individuals;
- The definition of "substantial harm or inconvenience;" and
- The definition of Sensitive Customer Information.

As discussed in our first letter in response to the Commission's cybersecurity proposal for advisers,[9] we also recommend that the Commission not require advisers to disclose publicly, including through breach notifications, specific efforts they have taken to remediate a data breach. This is crucial to allowing them to protect themselves more effectively against threat actors. We believe that the potential risks resulting from public disclosure strongly outweigh any benefits.

D. Recordkeeping

We appreciate and share the Commission's view that periodic review and written documentation of the adviser's disposal practices generally should be sufficient to satisfy the proposed recordkeeping requirements as they relate to the disposal rule. We recommend that, in addition to the preamble, the text of any final rule include this specific language.

E. Cost-Benefit Analysis

We urge the Commission to undertake a more expansive, accurate, and quantifiable assessment of the specific and cumulative costs, burdens, and economic effects that would be placed on advisers by the proposed requirements, as well as of the potential unintended consequences for their clients.

F. Proposed Compliance Date

We recommend that the Commission provide a longer transition period that would take into account the several concurrent overlapping rule proposals discussed below, allow a more reasonable time for advisers to implement and operationalize changes, and prevent industry disruption.[10]

---

[9] *See* Letter from IAA General Counsel Gail C. Bernstein to the Commission re: *Cybersecurity Risk Management for Investment Advisers* (Apr. 11, 2022), available at https://investmentadviser.org/resources/comments-on-proposed-cybersecurity-rules-for-advisers/ (**First IAA Cybersecurity Letter**), in response to *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 (**Cybersecurity Proposal**).

[10] In light of the multiple rules that are likely to all be finalized at the same time and the short time provided for a thorough analysis of the potential implications of each of the relevant proposals, including as to their orderly implementation, it is difficult to provide a compliance period recommendation in a vacuum.

G. Holistically Addressing Rulemakings

The Proposal overlaps with, will be affected by, and will have implications for several other open Advisers Act rulemakings. The Commission should reopen the Outsourcing, Safeguarding, and Cybersecurity Proposals,[11] and keep the comment period for this Proposal open during that same time period, to consider and address their interrelationships and perform a holistic cost-benefit analysis.

H. Coordination with Other Federal Regulators

We believe that uniformity and consistency are critical in this area. We encourage the Commission to continue to collaborate with other federal financial regulators with a view to adopting uniform and consistent data protection approaches and data breach notification requirements.

II. Recommendations

A. The Commission should modify certain of the proposed safeguards to cover only Sensitive Customer Information.

As defined in the Proposal, Customer Information could include any information the adviser obtains about a client or prospective client,[12] while Sensitive Customer Information is Customer Information, alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information.[13]

We support the Commission's adoption of a rule that mandates advisers to establish written policies and procedures that address safeguards for client PII, including administrative, technical, and physical measures. However, we believe that certain of the proposed safeguards, including the incident response program and requirements related to Service Providers, should cover Sensitive Customer Information, and not Customer Information more broadly.

---

[11] *See* Cybersecurity Proposal; *Safeguarding Advisory Client Assets*, 88 Fed. Reg. 14672 (Mar. 9, 2023), available at https://www.govinfo.gov/content/pkg/FR-2023-03-09/pdf/2023-03681.pdf (**Safeguarding Proposal**); *Outsourcing by Investment Advisers*, 87 Fed. Reg. 68816 (Nov. 16, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-11-16/pdf/2022-23694.pdf (**Outsourcing Proposal**).

[12] The definition of "Customer Information" refers to nonpublic personal information in SEC Rule 248.3(t) that is defined as "[p]ersonally identifiable financial information." Personally identifiable financial information means "any information: (i) A consumer provides to [an adviser] to obtain a financial product or service from [an adviser]; (ii) About a consumer resulting from any transaction involving a financial product or service between [an adviser] and a consumer; or (iii) [An adviser] otherwise obtain[s] about a consumer in connection with providing a financial product or service to that consumer." 17 C.F.R. § 248.3(u).

[13] Proposed Rule 248.30(e)(9)(i).

As discussed more fully below, we do not believe it should be necessary for an adviser to implement policies and procedures to detect, respond to, and recover from unauthorized access to or use of all Customer Information, given the breadth of that definition. The Commission recognizes that the focus should be on Sensitive Customer Information in its proposed requirement to "[n]otify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization."[14] We agree that clients would view the protection of their Sensitive Customer Information as a critically important aspect of their relationship with their adviser, and believe that an adviser's efforts and resources should appropriately be focused on this information. We do not think, however, that the proposed requirements for broader Customer Information are proportionate to the attendant risks of their disclosure. Similarly, the proposed requirements relating to Service Providers that have access to any Customer Information are disproportionate to the benefits and risk presented.

B. The Commission should modify the Incident Response Program requirements.

1. The Commission should continue to allow advisers to use a principles- and risk-based approach to tailor their assessment and containment-and-control policies and procedures.

The IAA appreciates the Proposal's recognition that "given the number and varying characteristics (*e.g.,* size, business, and complexity) of [advisers], each institution needs to be able to tailor its incident response program based on its individual facts and circumstances."[15] We agree with the Commission's view that there should not be a one-size-fits-all approach to incident response programs, and that an adviser should have discretion to determine which elements are relevant to its business and how they should be implemented, and which are not necessary or appropriate. In this regard, we ask that any final rule make clear that specific steps for incident response are not required and expressly indicate that in developing their programs, advisers should employ a principles- and risk-based approach, under which controls are commensurate with risk.

We would oppose any requirement for an adviser to designate an employee with specific qualifications and experience (or hire a similarly qualified third party) to coordinate its incident response program. We appreciate that, while the Proposal includes a question on designation, it does not propose to require it.[16] Such a requirement would be onerous for smaller advisers, where employees generally wear multiple hats and that have too few personnel for it to be reasonable for the Commission to mandate a designated employee. Additionally, advisers of all sizes are already required to designate a chief compliance officer responsible for implementing compliance policies and procedures. There is no need to impose an additional specific designation for the incident response program. Similarly, the Commission should not require that

[14] Proposed Rule 248.30(b)(3)(iii) (emphasis added).

[15] Proposal, 88 Fed. Reg. at 20622. We urge the Commission to apply the same approach to its other rulemakings.

[16] Proposal, 88 Fed. Reg. at 20625, Q.16.

advisers hire a third party for this purpose. Instead, the Commission should allow advisers to decide whether a designated employee or third party is appropriate in light of their particular incident response program.

2. The Commission should narrow and clarify the definition of Service Provider.

a. Any final rule should only include Service Providers that receive, maintain, or process Sensitive Customer Information.

Under the Proposal, Service Provider is defined as "any person or entity that is a third party and receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to [an adviser]."[17] We believe the proposed definition of Service Provider is unrealistically and unnecessarily broad, reaching service providers where there are little or no marginal benefits to their inclusion and the costs (time, money, personnel, etc.) to advisers would be substantial.

As defined in the Proposal, customer information could include any information the adviser obtains about a client or prospective client. For example, under the Proposal, a scheduling app that obtains a client's name and unlisted telephone number could be a Service Provider. A mail processing service could be a Service Provider because it could obtain clients' names and addresses, with the knowledge that they are clients of the adviser.[18] A venue (conference hall, hotel, etc.) that provides facilities for a client seminar could be a Service Provider because it may obtain a client's name, email address, and unlisted telephone number. Capturing these types of situations would impose disproportionate burdens on advisers that are simply not justified by the potential risks and we do not believe this is the Commission's intention.

Adding a qualifier to the definition of "Service Provider" that the information be "sensitive" would appropriately narrow and clarify the range of third parties that potentially pose a material risk. It would also more closely track current practices. Instead of assessing all service providers in the same way, advisers today generally follow a risk-based approach and tier their service providers based on how closely they work with or have access to Sensitive Customer Information. Advisers prioritize those higher-risk service providers instead of spending resources (personnel, expertise, time, and financial) unnecessarily on service providers that do not receive or have access to Sensitive Customer Information.

As noted above, this change would also align with the customer notification provision of the Proposal, where advisers would be required to "[n]otify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used

[17] Proposed Rule 248.30(e)(10).

[18] Even if the client's name and address are deemed to be public information, which is not always the case, the fact that an individual is an adviser's client would be nonpublic.

without authorization."[19] Moreover, our suggested approach is consistent with the National Institute of Standards and Technology (**NIST**) framework cited by the Commission in the Proposal, which would likely not include third-party service providers that do not have access to the adviser's Customer Information System or those that only have access to limited information such as a client's name and/or telephone number.[20]

We offer the following alternative definition of "Service Provider" under proposed Rule 248.30(e)(10), marked to compare to the proposed definition:

> *Service provider* means any person or entity that is a third party and receives, maintains, processes, or otherwise is permitted access to sensitive customer information, as defined in Section 248.30(e)(9), through its provision of services directly to a covered institution.

b. The Commission should exclude certain categories of service providers from the definition of Service Provider.

We recommend that the Commission exclude certain categories of service providers from the definition of "Service Provider" because they generally do not raise the concerns underpinning the proposed definition. Specifically, the Commission should exclude affiliated service providers operating under a shared services or similar model and entities subject to the GLBA that have direct contractual relationships with the client.

i. Affiliated service providers operating under a shared services or similar model.

The Proposal treats an adviser's affiliate that provides services to the adviser as a Service Provider.[21] For the same reasons we offer in our supplemental letter on the Commission's Outsourcing Proposal,[22] the IAA believes that it is neither appropriate nor necessary to treat affiliates that provide services to an affiliated firm through a shared services or similar model as Service Providers. Many advisers are structured in a manner that makes it administratively beneficial for them to obtain services from affiliates. These services often are provided by affiliates in a manner established by the organization's policies without the need for formal

---

[19] Proposed Rule 248.30(b)(3)(iii) (emphasis added).

[20] The NIST framework defines key cybersecurity supply chain risks as risks from third-party service providers "with physical or virtual access to information systems, software code, or [intellectual property]." *See* NIST, *Best Practices in Cyber Supply Chain Risk Management, Conference Materials*, available at https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf.

[21] Proposal, 88 Fed. Reg. at 20626.

[22] *See* Letter from IAA General Counsel Gail C. Bernstein to the Commission re: *Outsourcing by Investment Advisers* (Apr. 20, 2023), available at https://investmentadviser.org/resources/iaa-submits-supplemental-letter-on-outsourcing-proposal/ (**IAA Supplemental Outsourcing Letter**).

contracts because the affiliates are typically subject to company-wide policies and standards relating to safeguarding PII. Moreover, the information security policies of affiliates are typically subject to oversight by an organizational component that monitors compliance.

The Proposal would require that affiliate Service Provider arrangements be subject to oversight with respect to each entity in the same organization to which the affiliate provides services. This approach misperceives the nature of how advisers interact with affiliates and is also unwarranted given the nature of these affiliate arrangements. We see no purpose to be served by requiring an adviser to exercise this type of oversight of its affiliates. The Commission itself recognizes the unique relationship between affiliates in another section of Regulation S-P. SEC Rule 248.13(a)(1) establishes an exception from the opt-out requirements for information disclosures to affiliates that provide services to advisers,[23] implicitly acknowledging that there is little reason to treat affiliates as Service Providers. This should especially be the case where affiliates operate under a shared services or similar arrangement.

ii. Separate entities subject to the GLBA that have direct contractual relationships with the client.

The Commission should eliminate the potential for confusion as to the level of oversight that must be applied in those instances where two distinct entities, both of which are subject to the GLBA, provide services to shared customers on a concurrent basis.

For example, an adviser's clients establish accounts with a custodian. In this context, both the adviser and custodian have concurrent relationships with the client. Through those separate relationships, the shared client independently and directly gives the adviser and custodian access to the client's PII. The same is true for an adviser's clients that separately contract with other entities subject to the GLBA, such as sub-advisers ("dual contract" sub-advisory relationships), insurance companies, tax and accounting firms, and certain mortgage companies (together with custodians, **GLBA Entities**).

Each GLBA Entity has its own independent regulatory obligations under the GLBA, including providing the client with a separate privacy notice, and would be subject to its own Regulation S-P or state data breach laws. Given that both the adviser and the GLBA Entity would each be obliged to comply with information security requirements, it would be unnecessarily duplicative for either to be subjected to oversight by the other under the proposed Service Provider construct.

[23] Similarly, current Commission rules permit covered institutions with related entities covered by privacy requirements under Regulation S-P and other GLBA regulations to provide joint notices. *See* Regulation S-P, sections 248.9(f) and (g).

c. The Commission should not require advisers to enter into written agreements with Service Providers.

We strongly support requiring reasonable oversight of Service Providers as part of an adviser's fiduciary and compliance responsibilities, including with respect to safeguarding Sensitive Customer Information. We have expressed similar support for adviser oversight in many of the other open Commission proposals.[24] In our responses to those proposals, however, we have also repeatedly expressed strong concerns about the infeasibility of negotiating contracts with or obtaining written assurances from service providers – and thus the likely ineffectiveness of such requirements.[25] Yet the Commission continues proposing to mandate them, and this Proposal, once again, would require an adviser to negotiate written contracts with its Service Providers that commit the Service Providers to take specific measures they may not otherwise be required to take and that the adviser may not have the leverage to force them to take.[26]

Specifically, under the contract, Service Providers would be required to take appropriate measures that are designed to protect against unauthorized access to or use of Customer Information. These include notification to the adviser as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security resulting in unauthorized access to a Customer Information System maintained by the Service Provider. This requirement is designed to enable the adviser to implement its incident response program. We do not disagree that Service Providers should protect Sensitive Customer Information and be required to provide timely notification of a breach to the adviser, but mandating this by contract simply will not work for all advisers.

As we discussed in other recent comment letters, many entities that would be service providers under those or this Proposal are unwilling to negotiate with their customers, including when those customers are investment advisers. Advisers increasingly engage service providers – especially large service providers – through a take-it-or-leave-it "click-through agreement" or

---

[24] *See, e.g.*, Letter from IAA General Counsel Gail C. Bernstein to the Commission re: *Outsourcing by Investment Advisers* (Dec. 23, 2022), available at https://investmentadviser.org/resources/iaa-letter-to-sec-on-service-provider-outsourcing/ (**First IAA Outsourcing Letter**); IAA Supplemental Outsourcing Letter; First IAA Cybersecurity Letter.

[25] *See, e.g.*, First IAA Outsourcing Letter; IAA Supplemental Outsourcing Letter; First IAA Cybersecurity Letter; Letter from IAA General Counsel Gail C. Bernstein to the Commission re: *Private Fund Advisers* (Apr. 25, 2022), available at https://investmentadviser.org/resources/iaa-letter-to-sec-on-private-fund-advisers-proposal/; Letter from IAA General Counsel Gail C. Bernstein to the Commission re: *Safeguarding Advisory Client Assets* (May 8, 2023), available at https://investmentadviser.org/resources/iaa-letter-to-sec-on-safeguarding-advisory-client-assets-proposal/.

[26] *See infra*, note 50. Consistent with current law, advisers generally do not have contracts with affiliated service providers today. They also may only have contracts with nonaffiliated service providers in limited circumstances, such as joint marketing arrangements, but not more broadly for services and transactions carried out in the ordinary course of business. *See* 17 C.F.R. § 248.13, 14. Under the GLBA, written agreements with Service Providers are only required where the services provided are not provided by an affiliate and are other than for processing and servicing transactions.

addendum in which an adviser agrees to accept a service provider's terms (including its information security measures) with no opportunity to negotiate those terms. Even when a more traditional contract is presented, we understand that individual advisers (particularly smaller advisers)[27] lack leverage to engage in contractual negotiations with many service providers. In the rare instances that service providers agree to negotiate terms, advisers of all sizes, and particularly smaller advisers, lack leverage to require specific terms, especially when those terms expose service providers to potential liability, and especially when those service providers are not regulated by the Commission. Given our members' experience, we believe it is highly unlikely that service providers, including those that would be Service Providers under this Proposal, will voluntarily enter into legally binding contracts with advisers, as contemplated by the Proposal, when they are not otherwise required to do so.

We do not understand in these cases how an adviser can be expected *under any of these proposals* to require service providers to include specific contractual language or provide specific written assurances. For example, while advisers need to be informed of a data breach at a Service Provider without unreasonable delay, we do not believe that Service Providers, for the most part, will contractually agree to bind themselves to providing that notice within 48 hours under all circumstances. Moreover, depending on the scale and nature of a Service Provider's business, the Service Provider may not permit separate "oversight" of its information security policies by a third party. This concern applies equally to service providers under the other proposals discussed herein. Moreover, as with other Commission proposals, we have serious concerns about the Commission's use of the Advisers Act to turn advisers into the guarantors of their Service Providers' information security programs as proposed here.

Even if Service Providers agreed to enter into written agreements with advisers as proposed, advisers and Service Providers would both likely incur significant negotiation and implementation costs,[28] which we do not believe are justified, especially when an alternative and less burdensome approach is available.

---

[27] The median number of non-clerical employees of SEC-registered investment advisers was eight at the end of 2021, with 58 percent of SEC-registered advisers having fewer than 10 non-clerical employees and 88.1 percent having fewer than 50 non-clerical employees. *See IAA-NRS Investment Adviser Industry Snapshot 2022* (June 2022), available at https://investmentadviser.org/wp-content/uploads/2022/06/Snapshot2022.pdf.

[28] *See infra*, note 49. As discussed below, the Commission's economic analysis severely underestimates the costs and burdens of the Proposal on advisers. Moreover, in addition to the direct legal and operational costs incurred, the Proposal could result in barriers to entry and consolidation pressure, especially for newer or smaller advisers. We believe that these costs, whether direct or indirect, would outweigh the benefits.

In addition, the multiple requirements across proposals to enter into and renegotiate contracts or obtain written assurances, if adopted, will likely have different effective and implementation dates, forcing advisers to keep re-opening and renegotiating contracts, often with the same parties. For example, depending on how the Commission ultimately defines "Covered Function" in the Outsourcing Proposal, we would expect that many of those functions, for which written assurances would be mandated, would also require service providers to access client PII, thus mandating additional negotiation of written terms under this Proposal. *See generally* Cybersecurity Proposal; Safeguarding Proposal; *See Private Fund Advisers; Documentation of Registered Investment Adviser Compliance*

In our view – and as we have recommended in other contexts – an effective alternative to a required written agreement would be to allow advisers to tailor their oversight of their Service Providers based on the nature and size of their businesses and in light of the risks posed by the facts and circumstances, *i.e.*, through a risk-based and principles-based internal controls approach. We agree that contractual terms may be one effective way for advisers to oversee their Service Providers, but it is not the only way and advisers should be given the flexibility to adopt a process that works effectively for their circumstances. Accordingly, we would not object to the Commission's suggesting in the adopting release that, to the extent feasible and warranted by the adviser's risk assessment, the adviser could consider entering into or updating its contracts with its Service Providers to address any information security and data breach reporting concerns.

As discussed above, although we have pointed out similar practical and operational hurdles and made similar recommendations in other recent comment letters, the Commission continues to propose similar requirements without sufficiently crediting the difficulties advisers of all sizes, and smaller advisers in particular, will face. We have also previously recommended in other contexts, and reiterate here, that the Commission could look to its recent T+1 Final Rule,[29] in which it recognized the need for a more flexible approach than mandating a written contract, and provided that, instead, a broker-dealer could choose to establish, maintain, and enforce written reasonably designed policies and procedures.

While we recognize that no rule can be completely effective against all bad actors, we believe that an internal controls approach would provide more flexibility and reduce compliance and operational burdens on advisers. Such an approach can evolve as circumstances warrant (*e.g.,* to mitigate the risk of a data breach), and is more likely to put advisers in a position to detect, prevent, and mitigate the risk from a bad actor. We strongly recommend that the Commission adopt an internal controls approach rather than requiring the proposed written agreement.

Should the Commission nevertheless require a written agreement rather than follow our recommended internal controls approach, we urge it to limit the requirement to those Service Providers that have physical or virtual access to an adviser's Customer Information System.[30] We also urge the Commission to recognize that even under these limited circumstances, contracts may not be feasible for all advisers or in all circumstances, and we ask that the standard

---

Reviews, 87 Fed. Reg. 16886 (Mar. 24, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-03-24/pdf/2022-03212.pdf.

[29] In the recently adopted final rule for shortening the settlement cycle, the Commission stated that "the Commission generally agrees that requiring policies and procedures as an alternative approach to compliance, separate from entering into written agreements, provides broker-dealers with more flexibility to achieve same-day affirmation" and that it is "providing broker-dealers with this discretion under the rule to allow broker-dealers to select the approach that best aligns with their existing business practices and customer relationships." *See Shortening the Securities Transaction Settlement Cycle*, 88 Fed. Reg. 13872, 13893-13894 (Mar. 6, 2023), available at https://www.govinfo.gov/content/pkg/FR-2023-03-06/pdf/2023-03566.pdf (**T+1 Final Rule**).

[30] As noted above, this would align with the NIST framework cited by the Commission in the Proposal. *See* NIST, *supra* note 20.

in any final rule include a "good faith" qualifier so that advisers that are unable to negotiate contracts with their service providers are not deemed to be in violation of the rule.

C. The Commission should modify and clarify the Customer Notification obligations.

We support the Commission's adoption of a rule that would require advisers to provide a clear and conspicuous notice to each Affected Individual whose Sensitive Customer Information was, or is reasonably likely to have been, accessed or used without authorization, subject to the following recommended modifications.

1. The Commission should modify and clarify the notification obligation trigger.

We note a lack of clarity in the Proposal related to what event triggers the notification obligation, which appears to be inadvertent. Under the Proposed Rule, the incident response program must include procedures for Affected Individuals to be notified when their "sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization."[31] The preamble is consistent with respect to the notification obligation trigger: "[u]nder the proposal, the access or use without authorization of an individual's sensitive customer information (or the reasonable likelihood thereof) triggers the customer notice requirement."[32] However, elsewhere in the Proposed Rule, the text states that an adviser "must provide the notice as soon as practicable, but not later than 30 days, after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred."[33] To avoid confusion, we request that the final rule text make clear that the notification obligation is triggered by unauthorized access to sensitive customer information. We suggest rule text below.

The Proposal would also require advisers to provide notice to Affected Individuals within 30 days after becoming aware of unauthorized access to or use of their information, unless the Attorney General of the United States informs the adviser, in writing, that the required notice poses a substantial risk to national security.[34]

We recommend a 45-day rather than a 30-day notification requirement to provide a more reasonable amount of time for advisers to perform investigation and risk assessments, collect the information necessary to include in client notices, and provide notices in complex cases. It will also better align with existing state requirements. As the Proposal recognizes, over half of state data breach notification laws do not specify a number of days to report a breach and a majority of those states that do require notification allow for 45-60 days for reporting.

---

[31] Proposed Rule 248.30(b)(3)(iii).

[32] Proposal, 88 Fed. Reg. at 20670 (emphasis added).

[33] Proposed Rule 248.30(b)(4)(iii) (emphasis added).

[34] Proposed Rule 248.30(b)(4)(iii).

We also believe that the proposed law enforcement exception is too narrow and urge the Commission to allow for delayed notice for broader law enforcement purposes than proposed. We are concerned that the lack of a broader law enforcement exception would contradict the Commission's goal to establish a federal minimum standard for data breach notifications.[35] As the Commission itself notes, almost all states and other Federal financial regulators allow for delayed notification for law enforcement purposes.[36] Additionally, limiting the law enforcement exception as proposed could create broader security risks for clients and advisers, and we also do not believe that an adviser should be forced to choose between disregarding a law enforcement request, potentially with legal consequences for the adviser, or violating the rule.

Based on the discussion above, we offer the following alternative language for "Timing" under proposed Rule 248.30(b)(4)(iii), marked to compare to the proposed language:

> *Timing.* A covered institution must provide the notice as soon as practicable, but not later than ~~30~~ 45 days, after becoming aware that unauthorized access to or use of sensitive customer information has occurred or is reasonably likely to have occurred. The notification required by this section may be delayed beyond 45 days if a law enforcement agency determines that the notification will pose a significant security risk or impede a criminal investigation. The notification required by this section shall be made within 30 days after the law enforcement agency determines that the risk has abated and notification will not compromise the investigation.~~unless the Attorney General of the United States informs the covered institution, in writing, that the notice required under this rule poses a substantial risk to national security, in which case the covered institution may delay such a notice for a time period specified by the Attorney General of the United States, but not for longer than 15 days. The notice may be delayed for an additional period of up to 15 days if the Attorney General of the United States determines that the notice continues to pose a substantial risk to national security~~.

2. The Commission should modify and clarify the scope of Affected Individuals.

The IAA supports having advisers provide notice to individuals whose Sensitive Customer Information resides in an adviser's Customer Information System that was, or was

---

[35] *See* 15 U.S.C. 6804(a) (directing the agencies authorized to prescribe regulations under title V of the GLBA to assure to the extent possible that their regulations are consistent and comparable); *see also* 15 U.S.C. 1681w(2)(B) (directing the agencies with enforcement authority set forth in 15 U.S.C. 1681s to consult and coordinate so that, to the extent possible, their regulations are consistent and comparable).

[36] *See, e.g.,* RCW 19.255.010(8); Fla. Stat. sec. 501.171(4)(b); *see also Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, 70 Fed. Reg. 15736 (Mar. 29, 2005).

reasonably likely to have been, accessed or used without authorization if it is unable to identify which specific individuals' Sensitive Customer Information has been accessed or used without authorization.[37] However, we believe the current proposed language is overbroad and confusing and we recommend that it be modified and clarified.

The Proposed Rule states that "[i]f an incident of unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred, but the covered institution is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization, the covered institution must provide notice to all individuals whose sensitive customer information resides in the customer information system that was, or was reasonably likely to have been, accessed or used without authorization."[38]

The language suggests that, even where the adviser is reasonably certain that the information of certain individuals on the system was not accessed, because it is not certain which of the other individuals on the system were affected, it must notify all clients on the system. We are concerned that this language is likely to cause advisers to notify all clients whose sensitive customer information resides on its system, even in situations where the adviser knows that certain clients were not impacted. For example, assume that an adviser has a financial professional whose laptop is stolen. The laptop is only able to gain access to that financial professional's own client files, but following its theft, the adviser is unable to determine which of the client files would be able to be hacked. In addition, all of the financial advisers' client files reside on the adviser's larger system. Under these circumstances, while the adviser cannot be certain which of the financial adviser's clients' information is realistically at risk, it is reasonably certain that not all clients on the adviser's system were impacted. In this situation, the adviser may believe that, because it is not able to make that identification, it would need to send out a notice to all its clients. While this would be unnecessarily burdensome for the adviser, it may also have negative consequences for clients. While over-notification may appear benign, it potentially creates risk for clients. As we have noted in other recent comment letters,[39] there is a risk that too much information can be overwhelming and lead to desensitization. This is a particular concern in the context of data breaches. If unnecessary notifications create a "boy-who-cried-wolf" atmosphere, the situation may be further exacerbated as clients may not take appropriate actions when they do receive appropriately targeted notifications.

We suggest the following modifications to simplify and clarify the definition of Affected Individuals under proposed Rule 248.30(b)(4)(ii), marked to compare to the proposed definition. We also believe this better aligns with the Commission's intent.

---

[37] Proposed Rule 248.30(b)(4)(ii).

[38] *Id.*

[39] *See* Letter from IAA General Counsel Gail C. Bernstein to the Commission re: *ESG Disclosures for Investment Advisers* (Aug. 16, 2022), available at https://investmentadviser.org/resources/comments-on-sec-proposal-to-enhance-esg-disclosures-for-investment-advisers-and-funds/; First IAA Cybersecurity Letter.

> *Affected individuals*. If an incident of unauthorized access to or use of sensitive customer information has occurred or is reasonably likely to have occurred, ~~but the covered institution is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization,~~ the covered institution must provide notice to all individuals whose sensitive customer information ~~resides in the customer information system that~~ was, or was reasonably likely to have been, accessed or used without authorization.

3. The Commission should modify and clarify the definition of substantial harm or inconvenience.

The Commission proposes that an adviser's incident response program be reasonably designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience. It is proposed that the term "substantial harm or inconvenience" be defined as "personal injury, or financial loss, expenditure of effort or loss of time that is more than trivial, including theft, fraud, harassment, physical harm, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or the misuse of information identified with an individual to obtain a financial product or service, or to access, log into, effect a transaction in, or otherwise misuse the individual's account."[40]

The IAA is concerned that the standard is ambiguous because it would treat any financial loss that is slightly above "trivial" as "substantial."[41] The IAA recommends that the standard be established at a level that is consistent with the usual meaning of the term "substantial." Accordingly, we request that the term "substantial harm or inconvenience" be defined as "personal injury, material financial loss, or significant expenditure of effort or loss of time."

The IAA agrees with the Commission's view that a change to an account number is not "substantial harm." We also appreciate that the Commission's example that accidental access by an employee to a client's records would not constitute substantial harm or inconvenience if there is no significant risk of misuse has been expanded to include employees of affiliates and service providers of the firm.

We note that whether harm to a client is substantial can be subjective and not necessarily known at the outset of a breach. Depending on the type and duration of the breach, and the resources, investment profile, and risks of a particular client, the amount of harm could vary greatly from client to client. It is thus important for the Commission not to second guess a

[40] Proposed Rule 248.30(e)(11).

[41] We addressed concerns with similar wording in the context of proposed disclosure under the Cybersecurity Proposal.

"substantial harm" determination made in good faith by an adviser under the facts and circumstances known at the time.

We offer the following alternative definition of "Substantial harm or inconvenience" under proposed Rule 248.30(e)(11), marked to compare to the proposed definition:

> *Substantial harm or inconvenience* means personal injury, ~~or~~ material financial loss, or significant expenditure of effort or loss of time ~~that is more than trivial~~, including theft, fraud, harassment, physical harm, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or the misuse of information identified with an individual to obtain a financial product or service, or to access, log into, effect a transaction in, or otherwise misuse the individual's account.

4. The Commission should modify and clarify the definition of Sensitive Customer Information.

Overbroad definition. We recommend that the Commission narrow the proposed definition of Sensitive Customer Information, which is proposed to be defined broadly as "any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information."[42] The Commission seems to acknowledge the potential overbreadth of this definition, and the attendant concerns about problematic false alarms.[43]

For example, we of course appreciate the sensitivity attached to an individual's Social Security number. However, it is unclear to us how some of the other proposed information, such as a routing number or electronic address, without more, could be regarded as Sensitive Customer Information. For example, we do not see how a bank routing number could by itself allow for client identification or provide access to a client's accounts. We suggest minor modifications to the rule text below.

Employee Information. While not proposed to be included, the Commission asks whether it should include employee information as Customer Information. We urge it not to do

---

[42] Proposed Rule 248.30(e)(9)(i).

[43] Proposal, 88 Fed. Reg. at 20669 ("In the proposal, 'sensitive customer information' is defined more broadly than in most state statutes … the increased sensitivity could lead to false alarms—cases where the 'sensitive customer information' divulged does not ultimately harm the customer. Such false alarms could be problematic if they reduce customers' sensitivity to data breach notices."). We voiced similar concerns in our First IAA Cybersecurity Letter, where a broad interpretation of the triggering event for reporting cybersecurity incidents would lead to significant overreporting and be counterproductive to the Commission's goals.

so.[44] We respectfully submit that any such requirement may expand Regulation S-P coverage beyond the Congressionally mandated authority provided in the GLBA. The GLBA protects customer information and does not authorize the regulation of PII relating to employees of advisers. Further, we do not believe that the rule is necessary to protect employee information because employees are already protected by state employment and privacy laws.

We are also concerned that, if employee information is included, any final rule would apply to all advisers regardless of whether such firms have customer information to protect. For example, advisers managing only institutional or corporate portfolios, with no individual clients, would be required to develop complete incident response programs solely because such firms have employees. A number of advisers have no clients that are natural persons and are not otherwise covered by the GLBA and we do not believe extending the Proposed Rule to them would be justified. The Commission also has not accounted in its cost-benefit analysis for the likely substantial costs that would be imposed on these advisers. Nor has the cost-benefit analysis accounted for the significant costs on advisers that already have safeguarding policies and procedures. These firms very likely have not designed their programs to apply to employee information, which is subject to other protections and would likely require distinct policies and procedures.

Encrypted Information. We appreciate the Commission's recognition that encrypted information should not be regarded as Sensitive Customer Information because the risk of misuse of such information is virtually non-existent.[45] We agree that any information that is encrypted should not be regarded as Sensitive Customer Information unless there is reason to believe that the encryption key has been compromised or that the encryption method is outdated and ask that language to this effect be included in final rule text.[46] To address the Commission's concerns related to outdated technology, we would suggest adding "industry-standard encryption methods and capabilities" to prevent advisers from deploying out-of-date encryption programs

---

[44] Proposal, 88 Fed. Reg. at 20638, Q.78. The Commission asks whether any final rule should extend to employees' PII.

[45] The Commission states that "[g]iven the computational complexity involved in cracking the cipher texts of modern encryption algorithms generally viewed as secure, the compromise of cipher text produced by such algorithms in accordance with secure procedures would generally not give rise to 'a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information.' It would thus not constitute 'sensitive customer information,' meaning that the threshold for providing notice would not be met and thereby rendering an explicit encryption safe harbor superfluous in such cases." Proposal, 88 Fed. Reg. at 20674.

[46] The Commission seems to support this assertion. When speaking to the examples of Sensitive Customer Information, the Commission notes that "[w]hile the information cited in these examples is sensitive customer information, when that information is encrypted, it would not necessarily be sensitive customer information … Accordingly, in certain circumstances, information that is an encrypted representation of, for example, a customer's Social Security number may not be sensitive customer information under the proposed definition." Proposal, 88 Fed. Reg. at 20629, n. 112. This approach is also consistent with numerous state laws that regard information as sensitive personal information only if it is unencrypted. *See, e.g.*, California Information Practices Act of 1977, California Civil Code §1798.29(e).

and from using deficient encryption procedures.[47] If the Commission decides not to include encryption in the rule text, at a minimum, the Commission should affirmatively acknowledge that encryption is a factor that advisers may take into account in determining whether an incident will result in substantial harm or inconvenience.

Based on the discussion above, we offer the following alternative definition of "Sensitive Customer Information" under proposed Rule 248.30(e)(9)(i), (ii)(A) and (B), marked to compare to the proposed definition:

> (ii) Examples of sensitive customer information include:
>
> …
>
> (3) A unique customer electronic identification number, address, or routing code;
>
> …
>
> (iii) Sensitive customer information would not include encrypted customer information that renders the information unreadable or unusable, unless the covered institution reasonably believes that the encryption key has been compromised or the covered institution is not using industry-standard encryption methods and capabilities.

5. The Commission should not require advisers to disclose specific efforts they have taken to remediate a data breach.

As noted above, advisers would be required to notify affected clients after a data breach. As part of the notification, the adviser would need to describe the incident in general terms and specific information related to what the adviser has done to protect the sensitive customer information from further unauthorized access or use.[48] Similar to the concerns we expressed in our First IAA Cybersecurity Letter, we have serious concerns that the proposed specific disclosure notifications related to a data breach an adviser has suffered would be extremely useful to threat actors and not particularly useful to clients.

Moreover, as we also noted in our First IAA Cybersecurity Letter, this proposed specific disclosure could, in many cases, lead a client to reach unjustified and perhaps even misleading conclusions about an adviser's cybersecurity preparedness and thus not continue to engage an adviser that otherwise is highly suitable for its investment goals and whose data safeguards are

[47] For example, using the Advanced Encryption Standard (AES), the algorithm trusted as the encryption standard by the U.S. government. The AES standard is also used by Microsoft and Apple on their devices and in their applications.

[48] Proposed Rule 248.30(b)(4)(iv)(a).

robust. This is compounded by the likelihood that the adviser will have already remediated the vulnerability, making the information even less relevant to a client's decision. Additionally, as noted above, receiving unnecessary or unnecessarily detailed data breach notifications can be overwhelming and lead to counterproductive desensitization.

For the same reasons discussed in our First IAA Cybersecurity letter, we believe that a more targeted approach with respect to the level of required disclosures would more effectively achieve the Commission's goal of providing decision-useful information to clients while addressing our concerns above. More targeted disclosure would make it more likely that clients would read and understand the information being provided – *i.e.*, it would not overload clients with overly-detailed and hard-to-understand technical details – while reducing the chances of clients making inaccurate assessments, and, of crucial importance, providing threat actors with a detailed roadmap for further attacks.

We offer the following modification to the "Notice Contents" under proposed Rule 248.30(b)(4)(iv)(B), marked to compare to the proposed language:

> (iv) *Notice contents*. The notice must:
>
> …
>
> (B) ~~Describe~~ Provide a high-level description of what has been done to protect the sensitive customer information from further unauthorized access or use;

D. <u>The Commission should clarify an adviser's disposal recordkeeping obligations under the Proposed Rule.</u>

We appreciate and share the Commission's view that periodic review and written documentation of the adviser's disposal practices generally should be sufficient to satisfy the proposed recordkeeping requirements as they relate to the disposal rule. We recommend that, in addition to the preamble, the text of any final rule include this specific language, as follows:

> *Written policies, procedures, and records*. Every covered institution, other than notice-registered broker-dealers, must adopt and implement written policies and procedures that address the proper disposal of consumer information and customer information according to the standard identified in paragraph (c)(1) of this section. A covered institution's periodic review and written documentation of its disposal practices would generally be sufficient to satisfy the proposed recordkeeping requirements under this section.

E. The Commission should conduct a more accurate and holistic cost-benefit analysis, and in particular consider the disproportionate costs on smaller advisers.

We urge the Commission to undertake a more expansive, accurate, and quantifiable assessment of the specific and cumulative costs, burdens, and economic effects that would be placed on advisers by the proposed requirements, as well as of the potential unintended consequences for their clients. The Commission should consider, in particular, ways to ease the burdens of any final rule on smaller advisers, especially if the Commission does not accept our recommendations to refine the Proposal. Smaller advisers have been significantly burdened by one-size-fits-all regulations – both in isolation and cumulatively – that effectively require substantial fixed investments in infrastructure, personnel, technology, and operations. We are concerned that these stressors and barriers will negatively affect smaller advisers' ability to continue to serve their clients.[49]

F. The Commission should provide a more reasonable and realistic transition period.

The Proposal provides an unreasonable and wholly unrealistic 12-month transition period. The Commission severely underestimates the time it would take to implement a final rule and the implementation costs and burdens that would be imposed on advisers,[50] especially in

---

[49] The IAA again urges the Commission to consider regulation holistically and assess the cumulative impact of regulation on investment advisory firms of all sizes, particularly on smaller advisory firms. It is incumbent upon the Commission to conduct robust cost-benefit analyses, not only of each regulatory proposal in isolation, but of their cumulative effects on advisers, their clients, and the financial services landscape more broadly. As we have noted before, we believe that investor protection would not be well served by the Commission's hastily proposing and adopting such a magnitude of regulations in such a short period of time. Executive Order 13563, "Improving Regulation and Regulatory Review" issued in 2011, which is supplemental to and reaffirms the principles in Executive Order 12866, "Regulatory Planning and Review," requires agencies to "tailor [their] regulations to impose the least burden on society, consistent with obtaining regulatory objectives, taking into account, among other things, and to the extent practicable, the **costs of cumulative regulations**." (emphasis added)

There can be no doubt that the costs of compliance – direct and indirect – rise with each regulation and directly impact the resources advisers have to invest in other aspects of their businesses, including the resources available for client-facing efforts. We recognize that as an independent regulatory agency, the Commission is not legally bound by the requirements in Executive Orders 12866 and 13563. However, the Commission has long recognized "that these principles represent accepted standards of good practice in conducting rulemaking proceedings." *See, e.g.*, Commission, Office of the Inspector General, *Rulemaking Process*, Audit No. 347 (July 12, 2002), available at https://www.sec.gov/about/oig/audit/347fin.htm.

[50] The Service Provider written agreement obligation is a good illustration. The Commission recognizes that "even in cases where service providers are willing to adapt processes and contractual terms to meet covered institutions requirements, the task of renegotiating service agreements could—in itself—impose substantial contracting costs on the parties. Contracting costs are likely to be most acute for larger covered institutions, which may have hundreds of contracts that would require renegotiation. These additional costs would likely be passed on to customers in the form of higher fees." Proposal, 88 Fed. Reg. at 20667. However, the Commission fails to address these costs in any meaningful way and is thus dismissive of them, stating that due to data limitations, it is unable to quantify or characterize in much detail the structure of these various service provider markets and that the Commission is unaware of any data sources that provide detail on the reliance of covered institutions on third-party service providers. *See id.* at 20663 and n. 409.

light of the many other recently adopted and pending rulemakings that will need to be implemented by advisers. We have serious concerns that the proposed transition period would substantially raise rather than minimize the risks that the Proposal seeks to prevent.

Twelve months would not be nearly enough time for advisers to get ready for a final rule and related amendments and align current practices with the new regulatory requirements. It is also out of line with more realistic periods provided in connection with earlier amendments to Regulation S-P. For example, the Commission granted a two-year grandfathering provision for existing service agreements in the Regulation S-P final rule.[51] Additionally, in 2004, when the Commission adopted amendments to Regulation S-P that related solely to the disposal of consumer report information, advisers were provided approximately (i) seven months to implement the amendments and (ii) 18 months to revise their existing contracts with service providers for services involving the disposal or destruction of consumer report information.[52] The 2004 amendments to Regulation S-P did not require an undertaking nearly as extensive or onerous as the current Proposal, which, as discussed above, will necessitate entering into or renegotiating all contracts with Service Providers.

To implement a final rule, advisers will need to holistically reassess their current service provider infrastructure and undergo the time-consuming and expensive process of negotiating terms with each Service Provider, re-evaluate their current policies, procedures, and practices in light of any new requirements, prepare for new and/or different client notification obligations, and create and implement modified written incident response program policies and procedures and recordkeeping requirements. This will entail working with outside counsel to draft policies and procedures, operationalizing (including through technology builds or modifications), testing, and tweaking the policies and procedures, and training personnel. All of this will be done against the backdrop of meeting ongoing compliance and operational obligations as well as implementing additional new rule requirements at the same time.

We urge the Commission to provide a more reasonable and realistic compliance period with a longer time to transition for smaller advisers.[53]

---

[51] 17 CFR. § 248.18(c).

[52] *Disposal of Consumer Report Information*, 69 Fed. Reg. 71321 (Dec. 8, 2004), available at https://www.govinfo.gov/content/pkg/FR-2004-12-08/pdf/04-26878.pdf.

[53] We appreciate that the Commission has proposed a staggered compliance date for smaller advisers in its recent Safeguarding Proposal. Specifically, the Commission provides that the compliance date would be one year following the rule's effective date for advisers with more than $1 billion in regulatory assets under management (**RAUM**) and 18 months for advisers with up to $1 billion in RAUM. *See Safeguarding Proposal*, *supra* note 11. While we do not believe that the Commission has provided sufficient time for any advisers under that proposal, we appreciate its consideration of the disproportionate burdens on smaller advisers and urge the Commission to continue to do so in all its rulemakings. We also urge the Commission to consider other ways to make implementation of new rules more efficient, effective, and fair, for example, by tiering compliance with specific types of requirements or staggering compliance within and among different rules. We will address this issue further in the letter we plan to file in response to the Commission's reopening of the Cybersecurity Proposal.

G. <u>The Commission should reopen the Outsourcing, Safeguarding, and Cybersecurity Proposals to consider and address their interrelationships and to perform a holistic cost-benefit analysis.</u>

To allow all interested parties to provide feedback on how the many concurrent proposals interact with one another, we urge the Commission to reopen the comment periods for the Outsourcing, Safeguarding, and Cybersecurity Proposals and keep the comment period for this Proposal open during that same time period. While the Commission acknowledges the potential interaction between Regulation S-P and the Cybersecurity Proposal and reopened the latter proposal, it does not adequately address how these proposals may overlap or interact with one another or with other rules and rule proposals. It is essential for the Commission to consider – and allow stakeholders to consider – and then to provide clear guidance to advisers on how to navigate overlapping, duplicative, or even inconsistent requirements.[54]

Without a comprehensive evaluation of how these proposals align and potentially conflict with one another, advisers will face significant challenges in understanding and implementing the resulting regulatory obligations. This could lead to confusion, inefficiency, and unintended compliance failures, undermining the intended goals of the rulemakings.

The following examples demonstrate the complexity of the interrelationships among the various rule proposals and highlight the challenges advisers are facing in trying to address the potential implications of each proposal, especially in the short comment time periods provided by the Commission.

- The Regulation S-P, Safeguarding, Outsourcing, and Cybersecurity Proposals will require advisers to enter into and renegotiate contracts or obtain written assurances, often with the same parties but with different requirements and different implementation deadlines, yet the Commission does not address how these proposals may overlap or interact with one another, or the substantial and unnecessary costs attendant to multiple negotiations and renegotiations with the same parties, each one shifting costs and liabilities in different ways between the parties.

- The Outsourcing Proposal appears to intend to exclude custodians because it is the client, not the adviser, that selects and ultimately contracts with the custodian. However, the Safeguarding and Regulation S-P Proposals would require contractual privity between the

[54] We are not alone in our concern. Indeed, the Antitrust Division of the U.S. Department of Justice submitted a comment letter to the Commission on April 11, 2023 in response to proposed rules relating to market structure changes, calling on the Commission to "carefully consider potential interactions among the Proposed Rules when preparing their final versions, planning for the rules' implementation timelines, and evaluating the actual effects of the rules once they go into effect. In particular, the Antitrust Division urges the Commission to ensure that the final rules, taken together, preserve the benefits to competition identified by the Commission in each of the rules' proposals." Comment of the Antitrust Division of the United States Department of Justice on File Nos. S7-29-22; S7-30-22; S7-31-22; and S7-32-22 (Apr. 11, 2023), available at https://www.sec.gov/comments/s7-29-22/s72922-20164065-334011.pdf.

adviser and the custodian the client has selected, which raises the question of whether that custodial relationship would now be covered by the Outsourcing Proposal (assuming it were considered a "covered function" under that proposal) despite the Commission's stated intent not to include these relationships.

Reopening these interrelated proposals will also allow the Commission to undertake a more expansive, accurate, and quantifiable assessment of the specific and cumulative costs, burdens, and economic effects that would be placed on advisers, as well as of the potential unintended consequences for their clients. Firms also will be better able to consider the potential implementation challenges and other impacts of the various proposals in a more holistic way. The IAA strongly supports balanced, effective investor-protective regulation. However, excessive, conflicting, or confusing regulations can impose significant compliance costs on advisers. These costs are not only inefficient but can also divert resources from investor protection efforts, potentially undermining the intended objectives of the proposals.

H. The Commission should continue to coordinate with other federal agencies towards a uniform data breach notification standard.

We appreciate the Commission's recognition that establishment of a federal breach notification requirement would satisfy state notice laws that provide exemptions for firms subject to such a requirement, which will help to a degree to reduce the confusion and notification burdens arising from the patchwork of state data breach notification requirements.[55] We have long pressed for a uniform preemptive federal approach to breach notification to address this issue, and appreciate the Commission's consultation with other federal agencies in this regard. We request that the Commission continue to work towards a uniform standard to simplify this patchwork of conflicting notices and requirements.

* * *

[55] All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have adopted an array of inconsistent data breach notification laws and regulations that add to the confusion and regulatory burdens. For example, most, if not all, state laws require reporting of a data breach to affected individuals and state attorneys general, but these laws differ from one another and from federal regulation in several respects, including the timing and content of the notice. As the Commission recognizes, "states differ in the types of information that, if accessed or used without authorization, may trigger a notification requirement … [and] also differ regarding a firm's duty to investigate a data breach when determining whether notice is required, deadlines to deliver notice, and the information required to be included in a notice, among other matters." Proposal, 88 Fed. Reg. at 20618.

We appreciate the Commission's consideration of our comments on this important Proposal. Please do not hesitate to contact the undersigned at (202) 293-4222 if we can be of further assistance.

Respectfully Submitted,

/s/ Gail C. Bernstein
Gail C. Bernstein
General Counsel

/s/ William A. Nelson
William A. Nelson
Associate General Counsel

cc: The Honorable Gary Gensler, Chair
The Honorable Hester M. Peirce, Commissioner
The Honorable Caroline A. Crenshaw, Commissioner
The Honorable Mark T. Uyeda, Commissioner
The Honorable Jaime Lizárraga, Commissioner
William A. Birdthistle, Director, Division of Investment Management