May 12, 2008

By electronic mail

Ms. Nancy M. Morris, Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information, File No. S7-06-08

Dear Ms. Morris:

The Investment Adviser Association[1] welcomes the opportunity to comment on the Commission's proposed amendments to Regulation S-P.[2] The proposal would revise Regulation S-P by imposing more specific requirements for safeguarding information and responding to information security breaches, broadening the scope of the information covered by Regulation S-P's safeguarding and disposal provisions, specifying documentation of compliance, and providing a new exemption from current notice and opt-out requirements for a representative who moves from one firm to another.

The IAA strongly supports the SEC's goal to prevent and address security breaches and to enhance security of customer information. However, we have serious concerns about the proposed rule. While we recognize the conceptual appeal of making privacy rules applicable to investment advisers more consistent with those of banking regulators and the Federal Trade Commission, we are concerned that the proposal will impose unnecessary and costly requirements on investment advisers.

Following is a summary of our concerns:

1. The proposal is overly prescriptive and will be costly to implement; the SEC should maintain the flexibility of the current rules for investment advisers.
2. The IAA recommends modifications to proposed elements of the rule.

[1] The Investment Adviser Association (formerly the Investment Counsel Association of America) is a not-for-profit association that represents the interests of SEC-registered investment adviser firms. Founded in 1937, the Association's current membership consists of over 500 firms that collectively manage in excess of $9 trillion in assets for a wide variety of individual and institutional clients. For more information, please visit our web site: www.investmentadviser.org.

[2] *Part 248 - Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information,* SEC Rel. No. IA-2712, File No. S7-06-08 (Mar. 4, 2008) (Proposing Release).

3. The proposed documentation requirements are excessive.
4. The SEC should modify the scope of information and persons covered under the proposal.
5. The IAA supports the proposed exemption for transitions of professionals with suggested modifications.
6. The SEC should provide adequate time for implementation.

Background

The Gramm-Leach-Bliley Act (GLBA) was enacted to ensure the privacy and security of non-public personal information relating to individual "consumers" who have dealings with financial institutions, including those consumers that become "customers" of such institutions. The GLBA authorized the SEC and other federal agencies supervising financial institutions to promulgate rules for that purpose. In 2000, the SEC adopted Regulation S-P pursuant to the GLBA, which implemented privacy notice requirements and restrictions on sharing "consumer" and "customer" non-public personal information.[3]

Regulation S-P requires financial institutions, including SEC-registered investment advisers, to adopt policies and procedures reasonably designed to ensure the security and confidentiality of customer records. The rule has two basic elements: first, to require financial institutions to provide an initial notice of their privacy policies and practices upon entering into a customer relationship and prior to disclosing nonpublic personal information about a consumer to a nonaffiliated third party; and second, to provide for the security of that nonpublic financial information. Advisers are required to deliver annual notices to customers with whom an ongoing relationship exists and to permit consumers, via an opt-out notice, to prevent disclosure of nonpublic personal information to certain nonaffiliated third parties. Compliance with Regulation S-P was mandatory as of July 1, 2001.

The Fair Credit Reporting Act (FCRA) was enacted to regulate consumer reporting agencies, to ensure the accuracy and fairness of credit and character information contained in consumer reports, and to protect the privacy of individuals who are the subject of consumer reports. Under FCRA, "consumer reports" are defined as communications from a consumer reporting agency containing credit, character or other personal information for use in determining an individual's eligibility for credit, insurance, employment, or other purposes. Until 2003, compliance with FCRA requirements was delegated to the Federal Trade Commission and certain federal banking agencies. FCRA was amended by the Fair and Accurate Credit Transactions (FACT) Act of 2003, which added to FCRA a requirement that the FTC, the federal banking agencies, and the SEC issue regulations ensuring that any person that maintains or possesses consumer information derived from "consumer reports" for a business purpose "properly dispose" of any such information. To implement this requirement, the SEC amended

[3] *See Privacy of Consumer Financial Information (Regulation S-P)*, Final Rule, SEC Rel. No. IA-1883, File No. S7-6-00 (June 22, 2000).

Regulation S-P in 2004 by adding a provision governing disposal of consumer report information.[4]

On October 13, 2006, Congress enacted the Financial Services Regulatory Relief Act of 2006 requiring certain agencies, including the SEC, to develop a model privacy form that is succinct, easily readable, and comprehensible to consumers.[5] The agencies proposed such a form last year and the proposal is still pending.[6] The SEC now proposes to amend its rules to impose more specific requirements for safeguarding information and responding to information security breaches and to broaden the scope of information covered by both the safeguard and disposal provisions authorized separately by the GLBA and the FACT Act.

1. The proposed amendments are unnecessary, costly, and burdensome for investment advisers

We respectfully submit that the proposed amendments are unnecessary, costly, and burdensome for investment advisers and that the flexibility of current privacy rules should be preserved.

Current Privacy Requirements for Investment Advisers

Reg S-P currently requires investment advisers to adopt written policies and procedures reasonably designed to ensure the security and confidentiality of customer records and information, protect against anticipated threats and hazards to the security or integrity of customer records and information, and protect against unauthorized access to or use of customer records and information that could result in substantial harm or inconvenience to any customer.[7] In proposing these requirements, the Commission specifically recognized that investment advisers should have the flexibility to tailor their policies and procedures to fit their own organization's specific circumstances:

> We have not prescribed specific policies or procedures that financial institutions must adopt. Rather, we believe it more appropriate for each institution to tailor its policies and procedures to its own systems of information gathering and transfer and the needs of its customers.[8]

---

[4] *Disposal of Consumer Report Information*, SEC Rel. No. IA-2332, File No. S7-33-04 (Dec. 2, 2004).

[5] Pub. L. 109-351 (Oct. 13, 2006), 120 Stat.1966.

[6] *Interagency Proposal for Model Privacy Form Under Gramm-Leach-Bliley Act*, SEC. Rel. No. IA-2598, File No. S7-09-07 (Mar. 20, 2007). The IAA's comment letter on this proposal is available at http://www.investmentadviser.org/public/letters/comment052907.pdf.

[7] 17 CFR 248.30(a)(3).

[8] Privacy of Consumer Financial Information (Regulation S-P), Securities Exchange Act Release No. 42484 (Mar. 2, 2000) [65 FR 12354 (Mar. 8, 2000)].

In adopting amendments to the rule in 2004, the Commission reaffirmed this flexible approach: "We continue to believe that this [flexible] approach is appropriate. Therefore, we are not proposing specific policies and procedures that all firms subject to the rule must implement."[9]

We believe the Commission also should consider the requirements of the investment adviser compliance program rule (Rule 206(4)-7 of the Investment Advisers Act) in assessing whether to expand the privacy rule for investment advisers. The compliance program rule requires investment advisers to implement written policies and procedures reasonably designed to prevent violations of the Advisers Act, to designate a chief compliance officer responsible for administering and enforcing such policies and procedures, and to review them each year. The SEC has construed this rule to include policies and procedures to safeguard the privacy protection of client records and information under Reg S-P.[10]

Since the adoption of Reg S-P in 2000, investment advisers have met their obligation to develop and maintain policies and procedures to safeguard customer information in ways that are tailored to their firms and the risks of inadvertent disclosure particular to their business operations. With the adoption of the compliance program rule in 2004, these policies and procedures are reviewed annually as part of each firm's obligation to review the effectiveness of its compliance program, often under the direction of the firm's chief compliance officer. The proposal would essentially establish a duplicative regime, as the requirements already in place are substantially similar to elements of the proposed rule, including requirements to designate a responsible employee, inventory and assess risks, design policies and procedures to address those risks, monitor and test the effectiveness of controls, train staff, and evaluate and adjust the information security program to reflect monitoring and testing, material business changes, and other circumstances.

We request the Commission to refrain from imposing an additional layer of specific and inflexible privacy requirements. The current investment adviser privacy rules, in combination with the broad obligations imposed by the compliance program rule, are adequate and appropriate to achieve the stated purposes of the proposal.

Nature of Investment Advisory Profession

There are more than 11,000 SEC-registered investment advisers, representing a broad spectrum of firms. The vast majority of investment advisory firms are small,

---

[9] *Disposal of Consumer Report Information*, SEC Rel. No. IA-2293, File No. S7-33-04 (Sept. 14, 2004) at p. 9.

[10] *See Final Rule: Compliance Programs of Investment Companies and Investment Advisers*, SEC Rel. Nos. IA-2204; IC-26299; File No. S7-03-03 (Dec. 17, 2003) at n. 21 and accompanying text ("An adviser's policies and procedures, at a minimum, should address…safeguards for the privacy protection of client records and information.").

unaffiliated businesses that have limited resources.[11] According to information filed with the SEC, 90 percent of all federally registered investment adviser firms have fewer than 50 employees and 68 percent (more than 7,000 firms) have ten or fewer employees.[12]

The diverse and small business aspect of the investment advisory profession suggests that the current flexible approach – that allows firms to follow SEC guidelines to tailor policies and procedures appropriate to their size, operations, and the nature of their clientele and business – is preferable to a one-size-fits-all regulation.

Costs Resulting from Proposal

The cost estimates prepared by the Commission underscore the conclusion that the costs of the proposal for SEC-regulated financial institutions are substantial. The estimates indicate that large firms would need to spend $172,732 and small firms would spend $18,560 to implement the required elements of the rule.[13] The SEC estimates that smaller firms would need to spend an additional $10,764 per firm per year and larger firms would spend $51,084 for ongoing compliance.[14]

The cost estimates are based on the numerous and extensive tasks required by the proposal, including: amending contracts with service providers, amending and drafting policies and procedures, setting up documentation systems, assessing a wide range of risks, training staff, and performing ongoing monitoring. In addition, advisers may have to revise and re-print their privacy notices as well as any documents that currently incorporate the privacy notice inasmuch as the proposed changes may be sufficiently significant to warrant a re-notice of the privacy policy.[15]

Based on the Commission's cost estimates of implementing the proposal, we respectfully suggest that the current privacy and other complementary compliance regulations for investment advisers are appropriate and reasonable.

Given these concerns, we submit that the better approach would be for the Commission to allow investment advisers to use the proposed regulations as guidelines

---

[11] More than 83% of SEC-registered advisory firms manage less than $1 billion in assets. *See IAA/NRS, Evolution/Revolution: A Profile of the U.S. Investment Advisory Profession* at 5-6 (Aug. 2007), available on our web site, at 6. Further, approximately 42% (4,484) of all investment advisers are not affiliated with any other financial industry entity. *Id.* at 9.

[12] *Id.* at 7.

[13] Proposing Release at 72-73.

[14] *Id.*

[15] We collected information last year from larger investment advisory firms and their affiliates indicating that the costs of printing and mailing revised privacy notices could range from $100,000 to more than $300,000 per mailing. Such firms estimate a range from $.09 cents for printing and mailing a new privacy notice to $.24 per package. Some estimates project an additional flat charge of $300-$1,500 per lot depending on quantity. These estimates do not include reprinting and revising other forms that currently include the privacy notice.

rather than required legal obligations. The Commission could also incorporate such guidance in interpretive guidance, CCOutreach materials or frequently asked questions.

2. The IAA recommends modifications to proposed elements of the rule

Should the SEC nevertheless impose specific additional guidelines on advisers, we submit the following comments and requests for modifications:

Designate an employee to coordinate the information security program

The SEC proposes that firms designate an employee to coordinate the information security program to foster clearer delegation of authority and address the disperse elements of the program throughout an institution.[16] This rationale does not apply to smaller firms, which should not be required to designate such an employee. Investment 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 information security program.

The Commission requested comment on whether the designated employee should be designated by name, position, or office. If the SEC determines to impose this requirement, we suggest permitting all three options for designation of the person who will coordinate the program.

Identify in writing reasonably foreseeable internal and external security risks

The SEC proposes to require firms to identify in writing all reasonably foreseeable internal and external risks that "could result" in unauthorized disclosure, misuse, alteration, destruction or other compromise of personal information and to design and implement safeguards to control the identified risks. This proposed requirement is overly broad. The potential risks that "could result" in disclosure, destruction or misuse are potentially limitless. Similarly, the need to safeguard against each and every risk should be weighed against its importance and likelihood. We respectfully suggest that the Commission inject a measure of *materiality* into this proposed requirement, similar to the risk-based analysis that advisers and their SEC examiners currently employ in their compliance programs.

Train staff to implement the program

The SEC should clarify that a firm may comply with the proposed provisions regarding training and supervision of staff as part of its compliance program, supervisory, human resource, or any other appropriate policies and procedures of the firm. Such procedures need not be in a separate information security program.

[16] *See* Proposing Release at 63.

Oversight of service providers

The proposal requires investment advisers to oversee service providers, defined as a person or entity that receives, maintains, or has access to personal information through provision of services directly to the adviser. Specifically, advisers would be required to take reasonable steps to select and retain providers capable of maintaining appropriate safeguards for the personal information at issue, and require service providers by contract to implement and maintain appropriate safeguards (and document such oversight in writing). The SEC "anticipates" that reasonable steps could include use of a third-party review of those safeguards, such as a SAS 70, SysTrust, or WebTrust report.

This requirement is exceedingly broad and burdensome. Advisers typically retain numerous service providers that may have access to personal information, including employees' personal information, such as providers of payroll, tax, accounting, legal, technology, compliance, and employee benefits services (*e.g.* retirement plans and health, life, and disability insurance), not to mention service providers related to the adviser's core investment management services, such as broker-dealers, banks, subadvisers, and portfolio and accounting system providers. Requiring an adviser to oversee each of these service providers' safeguarding policies and procedures would be burdensome and costly. Amending each contract with a service provider alone would involve a substantial effort. Further, we would strongly oppose any requirement that advisers obtain a SAS 70, SysTrust, or WebTrust report from each service provider. Insistence on such a report could disrupt ongoing relationships with service providers that do not conduct these reviews and result in increased costs to advisers.

Instead of requiring extensive oversight of service providers and amendment of all contracts, the SEC should provide general guidelines in the adopting release that suggest various options, such as a confidentiality agreement or certification. [17]

Procedures for responding to security breaches

The SEC proposes that firms' written policies and procedures include procedures to: (1) assess any incident involving unauthorized access or use and identify in writing what personal information systems and what types of personal information may have been compromised; (2) take steps to contain and control the incident to prevent further unauthorized access or use and document all such steps in writing; (3) promptly conduct a reasonable investigation and determine in writing the likelihood that the information has been or will be misused after the firm becomes aware of any unauthorized access to sensitive personal information; and (4) notify affected individuals as soon as possible if the firm determines that misuse of the information has occurred or is reasonably possible.

With respect to assessment, containing and controlling, and conducting a reasonable investigation of incidents, such steps constitute a normal expected business response to an incident. Indeed the SEC recognizes that "most institutions investigate

[17] The SEC provided similar guidance with respect to due diligence on providers of record destruction services under the disposal rule. *See* Disposal Release, *supra n. 4* at 6.

data security breaches as a matter of good business practice."[18] We question whether a federal rule is needed to establish formal written procedures and documentation of these commonsense steps. Again, issuance of general guidelines in this area would suffice.

Notice to affected individuals

The proposal requires a firm to notify affected individuals if it determines that an unauthorized person has obtained access to or used sensitive personal information and misuse of the information has occurred or is reasonably possible. We suggest a number of clarifications to this requirement.

Party providing notice. The proposed rule should permit firms to handle information security breaches and any required notices to affected individuals jointly with affiliates, service providers, and similar parties.[19] For example, if a breach relating to an adviser's client occurs at a custodian or broker, the adviser should have the flexibility to coordinate with the other party regarding notice. The parties could determine that a joint notice is most appropriate or that the adviser is in the best position to provide notice given its relationship with the client. The rule should avoid requiring multiple notices to one customer of the same incident from multiple sources. To that end, the rule should permit notice "as soon as reasonably practicable" instead of "as soon as possible" to provide firms with an opportunity to investigate incidents and coordinate responses with other relevant entities.

Notice trigger. The rule should better distinguish between simple customer servicing incidents and reportable security breaches with attendant notices. For example, if a customer's grandchild has obtained a family user name and password and is trying to access an account, appropriate notice should be provided to the customer as a servicing accommodation, but should not rise to the level of a security breach with federal notice requirements. The SEC needs to incorporate a proper level of materiality to any required notices.

Coordination with state notification laws. The IAA appreciates the SEC's statement that establishment of a federal breach notification requirement would satisfy many state notice laws that provide exemptions for firms subject to such a requirement.[20] We encourage the Commission to coordinate with states that do not currently provide such exemptions to advocate the sufficiency of the SEC's breach notification requirement to satisfy state law. As the SEC recognizes, the "patchwork of overlapping and sometimes inconsistent regulation has created a difficult environment for financial institutions' compliance programs." Accordingly, we request the Commission to

[18] Proposing Release at 53.

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

[20] Proposing Release at 64.

consider any other action it may take either alone or working with state authorities to simplify this patchwork of conflicting notices and requirements.

Notice to SEC on Proposed Form SP-30

The SEC proposes that advisers provide notice on Form SP-30 to the SEC as soon as possible after becoming aware of an incident in which there is a significant risk that an individual might suffer substantial harm or inconvenience or an unauthorized person has intentionally obtained access to or used sensitive personal information. We do not believe that advisers should be required to report security incidents to the SEC by written report.[21] For example, we understand that banking regulators permit informal notice by telephone.[22] If a written report is required, however, the SEC should make the following modifications.

Content and timing. Form SP-30 requires more detail than is necessary to meet the Commission's goal of quickly assessing whether an investigative or examination response is warranted. Advisers may not have sufficient information to fill out Form SP-30 as soon as they become aware of an incident. We suggest that the Commission limit the form to a simple initial notice (*e.g.* limited to items 1-4). We understand that only eight states require regulatory notice and only two of those states require a written notice to the state regulator, both with much simpler notices than proposed by the SEC.

Alternatively, the SEC could consider two parts to any written report. The first part should be a simple *notice* by a time certain (*e.g.* by 10 business days after discovering the occurrence). The notice would include a description of the time, location, nature of the breach, an estimate of the number of customers affected, and a name and contact information. Later, the SEC could require submission of a *report* answering additional questions, such as the firm's intended response to the breach (*e.g*. 60 days from discovery of the breach). The SEC could introduce a higher threshold of materiality before requiring the second report.

Notice trigger. We applaud the SEC's efforts to avoid requiring notice to the Commission for minor incidents and to focus on breaches with a greater likelihood for harm.[23] To that end, we suggest some important changes to the SEC's proposed notice trigger. We recommend the SEC clarify the language requiring a regulatory notification in section 248(a)(4)(v)(A) and (B) so that these two provisions are either *both* required (change "or" to "and" at the end of subparagraph A) *or* conform the language of both A and B to include the qualifier that the affected individual "might suffer substantial harm or inconvenience." Alternatively, the Commission should revise paragraph B to require that the "unauthorized person has intentionally obtained access to [*and*] used sensitive

[21] We note that the FTC does not require similar notice in its privacy regulations.

[22] *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, 70 Fed. Reg. 15736 at 15741 (Mar. 29, 2005).

[23] Proposing Release at 25.

personal information." These modifications will assist in avoiding unnecessary or immaterial reports to the SEC.

Confidentiality. The SEC intends to afford confidential treatment to incidents reported on Form SP-30.[24] We strongly support this intent. The SEC should make every effort to maintain the confidentiality of the information in Form SP- 30, including protecting the information from FOIA requests.

3. The proposed documentation requirements are excessive

The SEC proposes to include specific documentation requirements with respect to virtually every element of its proposed standards for safeguarding and disposal programs, its proposed standards for responding to security breaches, and its transition of personnel exemption. The records required to be created and maintained under these regulations are daunting. For example, the proposal would require creating and maintaining a written record of an adviser's monitoring and testing, employee training and supervision, risk assessment, policy and procedure designs, and procedures related to assessment of security breach incidents. The proposal would require firms to document in writing that they are taking reasonable steps to select and retain service providers and requiring providers by contract to implement and maintain safeguards. The Commission's expectations regarding the level of detail imposed by these requirements are not clear.

The proposal would require advisers to maintain written records of information disclosed to departing representatives pursuant to the proposed exemption for information taken by a representative to another firm. Perhaps the most onerous documentation example is the requirement that an adviser "document in writing its proper disposal of personal information in compliance with the rule." This provision could be construed to require advisers to maintain a log describing each and every paper destroyed or to require advisers to obtain certifications from third-party service providers regarding each such paper. Investment advisers are already required to monitor and test the effectiveness of their policies and procedures under the compliance rule. Requiring documentation of each step in the process is unnecessary and burdensome.

The SEC should consider incorporating basic standards for maintaining certain types of documentation as part of its expected revisions to the investment adviser books and records rules. At a minimum, the Commission should provide guidance regarding the level of documentation it requires, including clarifying that firms may document compliance on a summary level rather than on an item-by-item basis. For example, SEC guidance could explain that an adviser's receipt and retention of certification by a record destruction company provides sufficient documentation of oversight and that the adviser need not require the company to provide a log of each record destroyed.

[24] Proposing Release at n. 55.

4. The SEC should modify the proposed scope of information and persons covered under Regulation S-P

Employees. Regulation S-P contains separate safeguarding and disposal provisions authorized by separate federal statutes with different goals and jurisdictional bases. The SEC now proposes to broaden the scope of information covered by both provisions without adequately considering whether such enhancements are authorized by the respective statutes. The proposal expands the information covered by the safeguard and disposal rules to protect "personal information," which would include any record containing "nonpublic personal information" under the GLBA or "consumer report information" under the FACT Act. In addition, "personal information" would include information "identified with any consumer, or with any employee, investor, or securityholder who is a natural person" that is handled by the firm or maintained on its behalf.[25] Thus, personal information would include personnel records of a firm's employees, including employee user names and passwords.

We respectfully submit that the proposal may expand Regulation S-P coverage beyond the congressionally mandated authority provided in the GLBA. The GLBA only protects customer information.[26] Nothing in the GLBA authorizes the regulation of non-public personal information relating to employees of financial institutions. Yet, one result of the proposed amendments is that advisory firms managing only institutional or corporate portfolios, with no individual consumers or customers, nevertheless would be required to develop complete information security programs solely because such firms have employees. A considerable number of advisers have no clients that are natural persons and would not otherwise be covered by the GLBA. These advisers are not required to have privacy policies and procedures because they have no customer information to protect.[27]

Further, the rule is not appropriately tailored to meet its stated objectives. The Commission reasons that safeguarding employee user names and passwords is important "because access to this information could facilitate unauthorized access to a firm's network and its *clients' personal information.*"[28] The SEC also recommends safeguarding personal financial information (including consumer report information) about employees "to reduce the risk that a would-be identity thief could *access investor information* by impersonating an employee" or using such personal financial information to bribe an employee into revealing such information. Thus, the stated intent of the

[25] We note that inclusion of employees in the definition of "personal information" may not work as a technical matter because the term references a definition (nonpublic personal information) that incorporates the "consumer" concept. "Consumer" as defined in Regulation S-P does not include employees.

[26] "Customer," as defined in Regulation S-P, only includes individuals.

[27] In fact, 28.3% (2,952) of advisers have no individual clients at all per their filings on the SEC's IARD system. *See Evolution/Revolution* at 10.

[28] Proposing Release at 32-33.

proposed amendments is to protect customer information. The proposal, however, would apply to all advisory firms regardless of whether such firms have customer information to protect.[29] Further, the rule is not necessary to protect employee information because employees are already protected by state employment and privacy laws.[30]

Finally, the rule would impose significant costs on financial institutions that already have safeguarding policies and procedures because many firms have not designed their programs to apply to employee information. For example, as noted above, the number of service providers subject to firm oversight expands exponentially if providers with access to employee information are included. In addition, the SEC has not accounted in its cost-benefit analysis for the substantial costs that would be imposed on firms that do not already have safeguarding policies and procedures because they have no customers.[31]

Supervised Persons. The SEC proposes to impose the requirements of the disposal rule on supervised persons of registered investment advisers. The Commission intends this amendment to make these persons "directly responsible" for proper disposal of information under their employers' policies and procedures. We oppose this requirement as redundant and unnecessary. Institutions can only act through their employees. Advisers are already responsible for the actions of their supervised persons and are subject to SEC sanction where violations are caused by their failure to supervise. The SEC should not take action that implies otherwise.

5. The IAA supports the proposed exemption for transitions of professionals with modifications

The IAA supports the proposed exemption from the notice and opt-out provisions of Regulation S-P to permit limited disclosure of customer information when firm personnel leave one firm and join another firm. The proposal strikes an appropriate balance between permitting clients to continue relationships while protecting sensitive information. We note, however, that investment advisers that hire new portfolio managers may need additional information to document performance results under SEC record-keeping requirements and/or Global Investment Performance Standards (GIPS). This type of documentation involves more than name, type of account, and contact information. We suggest the SEC provide relief for documentation sufficient to recreate

[29] The Commission could more appropriately tailor the rule to this intent by eliminating "employees" from its scope and instead provide guidance recommending that firms assess the risks presented by unauthorized access to certain employee information, such as user names and passwords, as part of their overall risk assessment.

[30] The FACT Act also covers disposal of "consumer report" information related to employees.

[31] *See* Proposing Release at 74 (stating that the proposed amendments to the scope of information covered by the rule would not require modification of firms' policies and procedures).

or verify investment adviser performance with appropriate protections for the information.[32]

The SEC proposes to limit its exception to information known to the employee at the date of separation. Sometimes, however, departures can be precipitous or unexpected. To the extent feasible, the SEC should permit the departing portfolio manager and the former firm sufficient time to resolve any issues related to documentation to be provided to the departing manager.

6. The SEC should provide adequate time for implementation

Advisers will require a significant amount of time to implement the proposed rule changes. For example, advisers will need to review, revise, and draft more specific policies and procedures, set up documentation systems, and fully assess a wide range of risks. In addition, review and amendment of contracts with service providers will require substantial time. Indeed, the SEC should consider a transition rule permitting amendments when contracts are renewed or renegotiated rather than revisions *en masse*. Further, the SEC should allow a sufficiently long period to facilitate a full cycle of revised annual privacy notices that would likely need to be given to customers. A phase-in period of at least 18-24 months would seem appropriate.

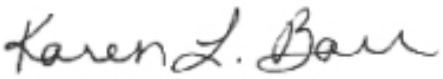
Further, we urge the SEC to coordinate implementation of all of its pending proposed changes to Regulation S-P including the SEC's 2007 proposed model privacy form. Advisers should be able to address all new privacy changes at the same time. Investment advisers should not have to complete this review and implementation process in multiple iterations with related notice requirements for customers.

[32] For example, the relief could specify that the information will be used by the new firm only in the aggregate to calculate performance results and that the new firm must protect the information fully pursuant to the requirements of Regulation S-P.

Conclusion

We appreciate the opportunity to provide our views on these important issues and would be pleased to provide any additional information the Commission or its staff may request. Please do not hesitate to contact Paul Glenn, IAA Counsel, or the undersigned with any questions regarding these matters.

Respectfully submitted,



Karen L. Barr
General Counsel

Cc: The Honorable Christopher Cox, Chairman
The Honorable Paul S. Atkins
The Honorable Kathleen L. Casey

Andrew J. Donohue, Director, Division of Investment Management
Robert E. Plaze, Associate Director, Division of Investment Management
Penelope Saltzman, Acting Assistant Director, Office of Regulatory Policy