INVESTMENT ADVISER ASSOCIATION

January 21, 2009

By electronic mail to David.Murray@state.ma.us

David A. Murray, General Counsel
Office of Consumer Affairs and Business Regulation
Suite 5170
10 Park Plaza
Boston MA 02116

Re: Public Hearings on "Standards for the Protection of Personal Information of Residents of the Commonwealth," *201 CMR 17.00*, held January 16, 2009

Dear Mr. Murray:

The Investment Adviser Association[1] welcomes the opportunity to comment on amendments extending time for compliance with the provisions of Code of Massachusetts Regulations at 201 CMR 17.00, originally promulgated as emergency regulations on November 14, 2008. By these amendments, the Office of Consumer Affairs and Business Regulation (OCABR) has delayed the effective date of this set of information security rules to May 1, 2009.[2]

The IAA supports the Commonwealth's goal of preventing and addressing security breaches and enhancing the security of its residents' personal information. We respectfully submit, however, that SEC-registered investment advisers already subject to extensive privacy regulations should be exempted from the requirements of the Massachusetts 201 CMR 17.00 regulations. In the absence of such exemption, we support the amendments extending time for compliance but also request additional time beyond May 1, 2009 to comply with the 201 CMR 17.00 regulations. Finally, we suggest that the Office of Consumer Affairs and Business Regulation post all comment letters and responses on its Web site for public review.

[1] The Investment Adviser Association (IAA) is a not-for-profit association that represents the interests of SEC-registered investment adviser firms. The Association's membership consists of investment advisory firms that manage assets for a wide variety of institutional and individual clients, including pension plans, trusts, investment companies, endowments, foundations, and corporations. Fifty-seven IAA member firms have headquarters in Massachusetts. For more information, please visit our web site: www.investmentadviser.org.

[2] The OCABR convened a hearing on the extensions-of-time amendments on January 16, 2009 and is accepting written comments until January 21, 2009.

1. Massachusetts should provide an exemption from 201 CMR 17.00 regulations for SEC-registered investment advisers.

SEC-registered investment advisers are subject to a strict fiduciary duty that requires maintaining the confidentiality of client information. In addition, such advisers are subject to extensive privacy requirements under federal law.

Congress enacted the Gramm-Leach-Bliley Act (GLBA) to ensure the privacy and security of non-public personal information relating to individual "consumers" who become "customers" of such institutions. In 2000, the SEC adopted Regulation S-P, which implemented the GLBA information safeguards and privacy notice requirements, as well as restrictions on sharing "consumer" and "customer" non-public personal information.[3]

Regulation S-P 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. In addition, advisers must 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. 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. Further, under Rule 206(4)-7 of the Investment Advisers Act (the compliance program rule), advisers are required to review their privacy policies and procedures annually to evaluate and address their effectiveness.

In addition, the Fair Credit Reporting Act (FCRA) protects the privacy of individuals who are the subject of consumer reports. FCRA was amended by the Fair and Accurate Credit Transactions (FACT) Act of 2003, which added to FCRA a requirement that the relevant federal regulators 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. The SEC implemented this requirement by amending Regulation S-P in 2004 to govern disposal of consumer report information.[4] In 2008, the SEC proposed amending its rules to impose even more specific requirements for safeguarding information and responding to information security breaches and to broaden the scope of information covered by both the safeguard

[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).

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

and disposal provisions authorized separately by the GLBA and the FACT Act.[5] This proposal is still pending.

Because SEC-registered investment advisers are already subject to an extensive federal regulatory regime governing protection of personal information, we respectfully submit that the Massachusetts requirements are not needed to protect Massachusetts clients of advisers and would impose unnecessary costs and burdens.[6] As your office and the Commonwealth of Massachusetts continue to consider further this legislation and its implementation, we strongly urge you to provide such an exemption.

2. Massachusetts should provide adequate time for implementation.

If advisers are not exempted from 201 CMR 17.00 regulations, they will require a significant amount of time to implement the new rules. The IAA supports and commends the OCABR for providing the current extensions of time for implementation, but requests a longer period of time for compliance. A phase-in period of at least 18-24 months would seem appropriate for the extensive requirements of the Massachusetts regulation.

For example, advisers will need to review and revise their policies and procedures to address specific Massachusetts requirements, identify and inventory information flows at the firm, fully assess a wide range of internal and external security risks, set up documentation systems, train staff, and perform ongoing monitoring. Most significantly, extensive time is needed to identify and implement new technology and any software and hardware upgrades needed to comply with the Commonwealth's far-reaching requirements regarding security procedures for computer systems, including wireless networks. Such efforts, both in time and cost, should be considered in light of the stressors of current economic conditions affecting the financial services industry. The Commonwealth should permit these costs to be incurred over a longer period of time.

Similarly, the Massachusetts regulation imposes exceedingly broad requirements on firms in overseeing their service providers and their use of appropriate technology to safeguard personal information, and to obtain certifications of compliance with Massachusetts requirements. 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 assure that each of these service providers adequately safeguards personal information consistent with the

---

[5] *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).

[6] The IAA is also concerned that the Commonwealth may seek to apply its regulatory requirements beyond its jurisdictional reach.

Commonwealth's requirements will involve substantial time and effort. Indeed, Massachusetts should consider a transition rule that would permit amendments to service provider contracts when contracts are renewed or renegotiated rather than revisions *en masse*.

3. The Office of Consumer Affairs and Business Regulation should post all comment letters and responses on its Web site for public review.

We understand that the OCABR has received numerous comment letters on this regulation and related hearings. We suggest that the OCABR post all comment letters and responses on its Web site for public review. The visibility and transparency of the OCABR deliberative process would be enhanced if members of the public could easily read and review each comment letter and any response from the OCABR or other Massachusetts official.

Conclusion

We appreciate the opportunity to provide our views on these important issues. We would be pleased to provide any additional information that the OCABR or its staff may request. Please do not hesitate to contact Karen L. Barr, IAA General Counsel, or the undersigned with any questions regarding these matters.

Respectfully submitted,

Paul D. Glenn
Counsel