IDC Independent Directors Council
Promoting Excellence in Fund Governance

ICI Strongly Opposes Massachusetts' Information Security Proposal, January 2008

January 10, 2008

Mr. Bryan Jamele, Legal Services Administrator
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116

Re: Proposed 201 CMR 17.00, Standards for the Protection of Personal Information of Residents of the Commonwealth

Dear Mr. Jamele:

The Investment Company Institute is writing to oppose strongly the Office of Consumer Affairs and Business Regulation's (the "Office") adoption of the proposed "Standards for the Protection of Personal Information of Residents of the Commonwealth," 201 CMR 17.00 (the "Standards"), which seeks to implement the provisions of the Massachu setts General Laws Chapter 93H.[1] The Institute is particularly concerned with the fact that the proposed Standards (1) seem to go far beyond what the Office's authority under Chapter 93; (2) are misguided in seeking to impose a "one-size-fits-all" and static approach to information security; and (3) sweep so broadly that they will have an extra-territorial impact that likely exceeds the Office's authority and offend Massachusetts' sister states. Each of these issues, and others, is discussed in more detail below.

As a preliminary matter, members of the Institute have long taken seriously their obligation to protect the confidentiality and integrity of non-public consumer information. Indeed, the report recently issued by the President's Identity Theft Task Force, Combating Identity Theft, noted that the federal regulator of the Institute's members, the U.S. Securities and Exchange Commission, "has actively examined securities firms to determine whether they have policies and procedures reasonably designed to protect their customers from identity theft. . . . The SEC has not yet found any deficiencies during its examinations that warranted formal enforcement actions." [2]

Because of the brevity of time provided to members of the public to comment upon the proposed Standards, our comments are not as specific or extensive as we would prefer. However, we trust they will convey the very serious concerns we have with the ultra vires nature of the proposal and the deleterious impact it will have on our members throughout the United States with shareholders who are residents of Massachusetts.

I. The Proposed Standards Exceed the Office's Authority under the Act

Primary among the Institute's concerns with the proposed Standards is the fact that, contrary to implementing the Chapter 93H, they attempt to wholly rewrite Chapter 93H's provisions. Indeed, as applied to the private sector, the law's provision is quite simple. It states in relevant part:

The department of consumer affairs and business regulation shall adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth. Such regulations shall be designed to safeguard the person information of residents of the commonwealth and shall be consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated. See Section 2 of Chapter 93H.

The privacy practices of the Institute's members, as registrants with the U.S. Securities and Exchange Commission, have been regulated under Title V of the Gramm-Leach-Bliley Act since its enactment. Such practices are additionally subject to the rules adopted by the SEC under the Act to implement its provisions. Our members, and other financial institutions subject to the GLB Act are precisely the types of entities that are referred to in the above provision. Accordingly, as applied to our members and other similarly situated entities, Massachusetts law requires that the regulations implementing Chapter 93H "be consistent with the

safeguards for protection of personal information" adopted by the SEC or the other federal regulators. And yet, contrary to this mandate, there is no provision in the proposed Standards that excludes or exempts federally-regulated entities from having the required "comprehensive information security program," including computer system security requirements. For some reason unknown to us, the proposed Standards completely ignore this statutory limit on the Office's rulemaking authority under Chapter 93H. At a minimum, to be consistent with the Office's authority under Chapter 93H, the proposed Standards need to expressly exclude federally-regulated financial institutions from their coverage.

II. The Proposed Standards are A Misguided Approach to Protecting the Personal Information of Massachusetts' Residents

Were we legally subject to the proposed Standards, we would be concerned with the fact that their proposed approach to computer security is very misguided. This is because the Office seems to be mandating a static, "one-size fits all" approach to its requirements, particularly those relating to computer security. While the Office's proposed computer security requirements appear to be based on the PCI Data Security Standards, it bears noting that such standards were developed for the payment card industry. Notwithstanding, this, the Office proposes to apply the standards developed for the payment card industry to all businesses and public entities without regard to the nature of such business or entity, its size, complexity, the types of records or information it collects and maintains, its information security needs, vulnerabilities, or existing system security, or the appropriateness of applying the payment card industry's standards to such entities. We are aware of no other provision under state or federal law that indiscriminately imposes on all businesses and public entities computer security system requirements of the nature proposed by the Offices. Indeed, even the regulations adopted by the federal regulators of financial institutions under the Gramm-Leach-Bliley Act take into account the nature of the financial institution and do not just cavalierly subject all federally-regulated institutions to identical requirements.

It also bears noting that, the more standardized security is, the easier it is to defeat, particularly on a large-scale basis. It is for this reason that, for example, the federal Department of Homeland Security has proposed to permit each nuclear facility in the United States to determine its own type and level of security rather than the Department imposing a "one-size-fits-all" standard on each such facility that, when compromised at one facility, is capable of being compromised at all facilities. It seems both inexplicable and naive that the Office would take a less enlightened approach to computer security. Instead, for those entities that will be subject to the Standards, the Office should ensure that its basis for such Standards is more principled and meaningful rather than taking a shortcut that subjects all entities to identical security standards without regard to their size, how critically sensitive their information, the extent of their vulnerabilities, and their resources.

Along these lines, we are quite confused by a provision in the proposed Standards that we recommend be addressed during the rulemaking process. This confusion derives from the language in proposed Section 17.03 that precedes the required contents of a "comprehensive information security program." While Section 17.03 lists, in detail, the required elements of a comprehensive information security program, this prefatory language provides that whether such program meets the requirements of the Standards "shall be evaluated" taking into account certain factors such as the size of the business, the amount of its resources, the amount of its stored data, and the need for the security and confidentiality of its data. If every entity has to establish a comprehensive information security program that, at a minimum, consists of the required elements set forth in Section 17.03, what is the purpose of this prefatory language? For example, at what point does it become relevant whether, in the Office's view, the entity has spent a sufficient amount of resources on its program [3] – and what expertise does the Office have to assess this? Either entities have to comply with each of the elements set forth in Section 17.03 or they do not. If they do, at what point are these additional factors relevant? Indeed, their mere inclusion seems, at best, contradictory to the requirements set forth in Section 17.03 and, at worst, an implication that, based on these factors, some entities may need to do more than the Standards require. To eliminate this confusion, we recommend that the Office delete this prefatory language.

III. The Proposed Standards would have Extra-Territorial Implications that Exceed Massachusetts' Authority

By their wording, the proposed Standards are limited in application to "every person that owns, licenses, stores, or maintains personal information about a resident of the Commonwealth." In our view, however, they need to be further limited in scope to ensure that they do not run afoul of Massachusetts' authority under Federal law and are respectful of the laws of the sister states of Massachusetts. Mutual funds are a perfect example to demonstrate the problematic reach of the proposed Standards. There are approximately 8800 mutual funds domiciled in the United States. It is not uncommon for these companies to have shareholders in a variety of states, if not in every state. Under the proposed Standards, a mutual fund located in California, or Texas, or North Dakota that has even one resident of the Commonwealth as a shareholder would be required to adhere to theproposed Standards with respect to that shareholder. To do so, the fund would have two choices: have separate and distinct information security policies for that one shareholder's information, [4] or apply the Standards to the entirety of its business.[5] Because the first option is impractical,

the fund's only practical choice may be to subject the entirety of its business to the Massachusetts Standards. California, however, may not agree with the Massachusetts Standards and determine to develop its own standards that, in their view, are superior to those of Massachusetts. What is our mutual fund to do in this situation? Is it expected to start segregating its shareholders based on their state of residency and employing the security practices of the variety of states where its shareholders reside? Such a result is both incredibly unrealistic and problematic. Most importantly, however, it would impede the ability of a nationwide business to conduct business efficiently and effectively on a nationwide basis. This is why Congress, in passing the Gramm-Leach-Bliely Act, deferred to the federal regulators of financial institutions to adopt regulations that would be uniform throughout the United States and not subject financial institutions to privacy regulations that differed by state. We strongly suspect that this consideration was also behind the wisdom of the General Court of the Commonwealth of Massachusetts when it expressly prescribed that, any rulemaking by the Office under Chapter 93H "shall be consistent with the safeguards for the protection of personal information set forth in the federal regulations by which the person is regulated."

We respectfully request that the Office heed the wisdom of the General Court and provide an express exclusion for federally-regulated institutions.

* * *

As noted above, the brevity of the comment period precludes the Institute from providing more detailed comments on our concerns with the specific provisions within the Office's proposed Standards and their related costs. However, we hope the above comments communicate our very serious and grave concerns with the proposal and why the Institute strongly opposes its adoption. We appreciate the opportunity to share our views with the Office and we hope our comments are given the utmost consideration by the Office during the rulemaking process.

If you have any questions concerning these comments, please contact the undersigned by phone (202-326-5825) or email (tamara@ici.org).

Sincerely,

/s/

Tamara K. Salmon
Senior Associate Counsel

Endnotes

[1] The Investment Company Institute ("ICI") is the trade association of the U.S. mutual fund industry. ICI seeks to encourage adherence to high ethical standards, promote public understanding, and otherwise advance the interests of funds, their shareholders, directors, and advisers. Members of ICI manage total assets of $12.70 trillion and serve almost 90 million shareholders. ICI members include 8,781 open-end investment companies (mutual funds), 665 closed-end investment companies, 428 exchange-traded funds, and 4 sponsors of unit investment trusts.

[2] See The President's Identity Theft Task Force, Combating Identity Theft, Volume II: Supplemental Information (April 2007) at p. 13.

[3] We are particularly troubled by the implication in this language that the Office believes it has legal access to the budgets of every entity – regardless of where located or domiciled – that maintains personal information on Massachusetts residents as well as the legal authority to determine that such entity is spending an appropriate amount of its resources on its comprehensive information security program.

[4] This is likely an impossible option based on the required elements of the program. For example, is the fund supposed to somehow inventory only those documents related this shareholder and conduct information audits of just this account?

[5] We believe that Massachusetts' sister states would be as offended as we are by the Office attempting to export its regulations into those states.