



Leadership is our business

Associated Industries of Massachusetts

222 Berkeley Street | P.O. Box 763

Boston, MA 02117-0763

www.aimnet.org | 617.262.1180 | fx 617.536.6785

May 12, 2009

**STATEMENT OF ASSOCIATED INDUSTRIES OF MASSACHUSETTS BEFORE
CHAIRMAN MICHAEL W. MORRISSEY, CHAIRMAN THEODORE C. SPELIOTIS
AND MEMBERS OF THE JOINT COMMITTEE ON CONSUMER PROTECTION AND
PROFESSIONAL LICENSURE IN SUPPORT OF S. 173, AN ACT ENSURING THE
PRIVACY OF CERTAIN DATA**

On behalf of Associated Industries of Massachusetts (AIM), the state's largest nonprofit, nonpartisan association of Massachusetts' employers, I am Bradley A. MacDougall, Associate Vice President for Government Affairs. Since the passage of 93H in 2007, AIM has been working with this Committee, the Administration, the Office of Consumer Affairs and Business Regulation and the Attorney General regarding the development of rules for the protection of personal information for residents of the Commonwealth. AIM appreciates and thanks the Administration for extending the general effective date of May 1, 2009 to January 1, 2010.¹ However, AIM members and individuals throughout the Commonwealth remain subject to highly prescriptive and costly rules that will have a significantly negative impact on our economic competitiveness. AIM supports S. 173, which would improve upon M.G.L. 93H through responsible and reasonable regulations for the protection and active security of personal information for residents of the Commonwealth.

AIM supports S. 173 because it will provide solutions for the Commonwealth's identity theft policies in the following ways:

- Provides consistency for entities that are already regulated under Federal law and regulations.
- Provides clear guidelines for the scope and development of identity theft regulations.
- Provides entities with an opportunity to invest their limited resources in a reasonable and strategic fashion to protect personal data according to their unique business models.
- Provides entities with an ability to enforce their data security policies on employees who willfully violate the Commonwealth's and the entities' data protection rules, regulations and policies.

AIM and our members believe that the protection of personal information is a necessary activity and an integral part of every business model. The business community and public agencies share

¹ The Federal Trade Commission also delayed the enforcement of Red Flag Rules until August, 1, 2009.

the same public policy goal and the many challenges of how to ensure the protection of personal data. Experts in data security continually struggle with the complex nature of technology and operational implications.

The public and private sectors have a lot to learn about the formulation and implementation of data privacy regulations. We have learned that this is not simple, yet the development of a reasonable public policy is vital for our economy. Our Commonwealth's economic competitiveness among its sister states and globally depends on technology, which serves as the neurocenter of commerce, and therefore the protection of personal data is essential. Massachusetts cannot afford additional unreasonable regulations on employers working to protect jobs and prevent layoffs.

Today, information and technology is the life-blood of our economy as services strive to meet customer demands in a global market place. Well before the Massachusetts legislature and Governor Deval Patrick enacted data security laws including 93H and 93I, many Massachusetts businesses identified data security as a top priority. Since that time, the business community has invested resources to address the many challenges related data security including employee training; technological, operational and legal solutions.

On November 19, AIM provided this committee with technical and business experts, who provided insights into the many complex issues surrounding data security. Members of the Committee learned from experts and business owners who urged more reasonable regulations. Clearly, "all persons" as regulated under 201 CMR 17.00 are not experts nor do all businesses have unlimited resources to hire additional staff or consultants to address the many legal and technology demands currently prescribed in the rules. AIM is committed to working with this committee, the Administration, the Attorney General and business leaders to develop a public policy that addresses our shared goal for a long-term solution to protect personal data.

Under current regulations, "all persons" and firms regulated cannot achieve 100% compliance because these regulations ignore the fact that many of the technological, legal and operational requirements are not readily available or reasonable for "all persons" or firms. In contrast to other states, the Massachusetts model is highly prescriptive, costly, lack clarity or recognition of federal regulations. Further, the regulations do not recognize the significant technological, legal, operational challenges or the significant investments and human talent required to address current regulations.

AIM has taken several steps to raise awareness, notify and educate our members and the broader business community about the new regulations. AIM has communicated with thousands of Massachusetts businesses and has provided hundreds of Massachusetts employers with education and resources through webinars and seminars throughout the state. AIM's seminars included industry experts, who provided human resources, legal, information technology and ongoing government affairs perspectives. The seminars raised general awareness, provided technical assistance and resources for businesses to analyze their data security protocols as prescribed under the 201 CMR 17.00. AIM also conducted several education seminars with members of Office of Consumer Affairs and Business Regulation. Even with this statewide outreach effort an overwhelming number of Massachusetts firms and "persons" are not fully aware of these new

regulations. Consistently, businesses indicate that AIM's communication and education seminars were the first time they were alerted to these new regulations.

AIM and its members remain concerned about the following issues related to 201 CMR 17.00:

Awareness and understanding: Most employers are unaware of these new regulations or mistakenly believe that if their firm is regulated by federal law then they are in compliance. These specific regulations represent a fundamental shift for every employer in Massachusetts and business transaction occurring within the Commonwealth. The challenge of compliance is further exacerbated by the regulation's ambiguity, which increases the risk of liability and affords little assurance that a business is in full compliance.

Data security is a priority: Employers want to implement effective tools and utilize resources to protect personal information. Yet, firms have limited resources and companies in Massachusetts are struggling to survive, retain employees, meet payroll and remain competitive in a global marketplace. Persons and employers should be provided the opportunity to apply reasonable efforts to protect personal data in both paper and electronic forms.

Education and third party vendors: Further, Massachusetts businesses are having significant challenges with educating, retaining and contractually binding vendors. Many firms that operate internationally have realized that the regulations do not envision the many national and global business relationships that they depend on.

Resources: AIM provided businesses with some helpful resources, guidelines and templates. However, the reality is that no template can be universally implemented because every business has unique data security needs. Therefore, many employers are frustrated with the confusing regulatory wording and the complexity of technological and legal issues. Firms are challenged by the extensive time, resources and expertise that is required to design and implement a data security program as outlined in 201 CMR 17.00.

Implementation: Many small firms lack the technical, legal and human resource capabilities to address the multidisciplinary nature of these regulations. As written, employers must invest in significant internal human resources and external consultants to address the legal and IT support needed to evaluate, upgrade and continually monitor their systems.

Highly complex and confusing: As currently written, these regulations are the most prescriptive set of laws and regulations in the nation. The rules go far beyond established federal standards, and will require in most instances significant operational and technological changes for entities that have custody of personal information, including employee records and customer data.

Significant ambiguity: The regulations place significant ambiguities into an already and evolving and complex discipline – data security. All companies cannot be 100% secure all of the time. There are over a 1.5 billion people with internet access and any of them can pose a danger. Technology, employee training and security practices are continuously evolving. While the regulations rely on a reasonableness standard and other components of consideration such as company size, resources available and the sensitivity of the data, the fact remains that every

person, 6.5 million residents of the Commonwealth plus any business that maintains or stores data of a Massachusetts resident, must abide by the minimum standards set forth by these regulations. Can every person effectively afford or access the resources and technical knowhow to understand or address these issues? Many firms are concerned that currently, the only opportunity they have to learn if their firm has achieved compliance is following an investigation by the Office of the Attorney General.

Public sector regulations: The regulations do not equally apply to the public sector. Therefore, can a firm continue to conduct business with the Commonwealth of Massachusetts if several state agencies do not accept encrypted data? Companies are concerned that the statute and the regulation would prevent them from sharing personal information with state agencies because said agencies do not accept encrypted data or may not provide a written certification.

Data security is not simple, no one person in a firm can provide the expertise and no one technological solution will provide security. We must get this right – cost effective data privacy rules that comply with the statute, set standards, recognize existing programs, and invite innovation.

Industry experts and business leaders have aggressively identified issues and are committed to help the administration formulate and examine solutions for the successful implementation 201 CMR 17.00. We respectfully urge the committee to give this matter a favorable report. We request that the Office of Consumer and Business Affairs carefully consider the significant and detrimental implications of these regulations and to utilize the intervening time prior to the effective date of May 1, 2009 to meet with the Office of the Attorney General and industry experts to address the current challenges with the regulations.

In closing, thank you for the opportunity to provide comments and I would be happy to answer any questions or provide additional information.