

Written Comments and Testimony Related to the January 16, 2009 Public Hearing on 201 CMR 17.00 Amendments

Table of Contents

Acme Cutrate Inc.....	4
Advantage Resolution Consulting	5
AICUM	8
American Insurance Association	12
Associated Industries of Massachusetts	20
Astron Inc.	29
Banas and Fickert Insurance Agency.....	30
Boston College	33
Burr Brothers Boats Inc.....	38
Business Coalition	45
Central Mass. Machine Inc.....	51
Chisolm Insurance Agency Inc.....	52
City of Revere	55
Cleary Insurance.....	58
College of the Holy Cross	61
CSW Inc.	64
DJ Kern	65
Eaton Vance Investment Managers	67
Energy Sciences Inc.	73
Fidelity Insurance	75
Fosta-Tek Optics, Inc.	80
Foster Insurance Agency Inc.	83
G.L. Gaudette III	86
Greater Boston Chamber of Commerce	89
Hayden Wood Insurance Agency Inc.	92

International Health, Racquet & Sportsclub Association..... 95

Investment Advisor Association..... 96

Investment Company Institute 100

Iron Mountain 151

James VanderBaan..... 152

John Hancock Life Insurance Company..... 154

Joint Committee on Consumer Protection and Professional Licensure 156

Life Insurance Association of Massachusetts 161

Madix, Inc..... 163

Massachusetts Association of Health Plans..... 164

Massachusetts Association of Insurance Agents 166

Massachusetts Bankers Association 172

Massachusetts Camping Association 175

Massachusetts Credit Union League..... 177

Massachusetts High Technology Council..... 183

Massachusetts Motor Transportation Association..... 185

Massachusetts Senior Care Association..... 188

MASSPIRG 190

McGrath Insurance Group Inc..... 191

Melick, Porter, and Shea LLP..... 194

Mental Health and Substance Abuse Corporations of Massachusetts, Inc. 197

Microsoft..... 199

MindSHIFT Technologies..... 201

National Federation of Independent Business 202

NetScout Systems, Inc..... 205

Northbridge Insurance Agency Inc..... 206

North Central Massachusetts Chamber of Commerce 209

O'Brien's Centerville Insurance Agency Inc..... 211

Paul Bowen 212

Property Casualty Insurers Association of America 213

Providers' Council 217

Retailers' Association of Massachusetts 219

Robert A. Peloquin Insurance Agency Inc. 223

Software & Information Industry Association 226

State Privacy and Security Coalition and National Business
Coalition on E-Commerce and Privacy..... 231

Symantec..... 238

Technology Association of America 239

Verizon 242

Wells Fargo..... 249

From: Jeff Fleming [jeff@acmecarpetone.com]
Sent: Tuesday, January 20, 2009 3:08 PM
To: Murray, David (SCA)
Subject: FW: re: data/security implementaion

From: Jeff Fleming [mailto:jeff@acmecarpetone.com]
Sent: Tuesday, January 20, 2009 2:45 PM
To: 'David.Murray@state.ma.us'
Subject: re: data/security implementaion

Office of Consumer Affairs and Business Regulation
Mr. David Murray
General Council

Thank you if you are reading this. We are a small business that tries to keep all consumer information private. This we have been doing for the last 40+ years. We are concerned with our ability to conform to the regulations that Massachusetts is going to require. We are not the size of Walmart, Target, TJMax, Home Depot; we are a small business of 11 people. The cost in money and time is giving these giant corporations a big advantage over us with their ability to have people and money to cover this. Please see what can be done to help really small businesses.

Jim Fleming, Acme Cutrate, Inc.

From: Molchan, Jor [jor.molchan@kewltechs.com]
Sent: Wednesday, January 21, 2009 11:31 AM
To: Murray, David (SCA)
Subject: Comments - 201 CMR 17.00 Hearing

January 21, 2009

David Murray
General Counsel
Office of Consumer Affairs and Business Regulation
10 Park Plaza
Boston MA 02116

RE 201 CMR 17

Mr. Murray,

Thank you for the recent hearing on 201 CMR 17. I was surprised that no consumer groups testified on behalf of consumer interests. Still, the recently announced Heartland Payment Systems breach underscores the importance of protecting consumer data. With or without this regulation businesses have an obligation to protect themselves and their clients from intrusion. 201 CMR 17 which codifies this responsibility should not be a surprise to any business in Massachusetts.

My specific comments follow;

Costs need not be prohibitive.

I am regularly surprised by the cost estimates that these businesses are providing. My firm is in the business of managing such compliance engagements. For small businesses compliance can be achieved for a fraction of the \$50,000 expense routinely cited.

While there is clearly work to be done many of the steps needed are common sense or part of good business practices.

Third Party Agents needs to be included

Deferring the third party agent requirement would eviscerate the law's impact. Any business which has access to confidential data needs to be managed. Outsourcing relationships are usually undertaken for cost savings. Managing this compliance is part of the outsourcing relationship.

Excluding third party agents is akin to locking the front door but leaving all the windows open.

Portable Devices needs to be included

Portable devices may be the most at risk portion of the business. Encryption or simply eliminating confidential data from such appliances is paramount.

Portable devices are easily lost or stolen beyond the physical controls of the office.

Specificity should not be expanded

Adding specifications to the law or further definitions may have the effect of diminishing protections for consumers. As written, business owners are responsible for making a judgment as to how to best protect the data they maintain.

Prescribing a specific remedy may assume a one size fits all solution or worse, define compliance by a standard that may be quickly outdated by future developments.

Awareness needs to be expanded

It is true that many businesses are not aware of 201 CMR 17. The Commonwealth should expand awareness to the business community as soon as possible.

This regulation sets important standards for the protection of consumers in Massachusetts. Further deferrals or reductions in its requirements will disadvantage consumers and expose them to further risk.

Jor Molchan
Managing Partner
Advantage Resolution Consulting
617 448 2225
jor@kewltechs.com

From: Murray, David (SCA) [David.Murray@state.ma.us]
Sent: Wednesday, December 03, 2008 1:25 PM
To: Molchan, Jor
Subject: RE: Enforcement - 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth

Mr. Molchan: The enforcement of 201 CMR 17.00 will be the responsibility of the Massachusetts Attorney General. Please let me know if we can be of any further help. Regards,

David A. Murray
General Counsel
Office of Consumer Affairs and Business Regulation
10 Park Plaza
Boston, MA 02116
(617) 973-8703
David.Murray@state.ma.us

From: Molchan, Jor [mailto:jor.molchan@kewltechs.com]
Sent: Wednesday, December 03, 2008 12:58 PM
To: david.murray@massmail.state.ma.us
Subject: Enforcement - 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth

December 3rd, 2008

Mr. Murray,

I am writing to understand enforcement of 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth. My firm is aware of GBLA upon which the act is based, and the enforcement role that the OCC and Fed play in that law. Regarding 201 CMR 17.00 we would like to understand which State of Massachusetts office will manage enforcement. Further, we would like to understand specifically, will the state conduct audits or reviews or require affirmative certification of compliance? This query is specific to cases prior to the occurrence of a breach. The Office of the Attorney General via Ben

Vitalini has advised that the law will be enforced by the OCABR. Desmond Berimondi of the OCABR has advised that the AG will enforce the law. Matt Huegel of the OCABR has directed me to your counsel. Your comments on the State's enforcement process are appreciated.

My interest is two fold as I manage my own business and assist other small business owners in their compliance with this important regulation.

Kind regards,

Jor Molchan
Principal
Advantage Resolution Consulting
617 448 2225



*Association of Independent
Colleges and Universities
in Massachusetts*

11 Beacon Street, Suite 1224 | Boston, Massachusetts 02108-3093
617.742.5147 | FAX 617.742.3089 | www.masscolleges.org

January 16, 2009

Daniel C. Crane
Undersecretary
Office of Consumer Affairs & Business Regulations
10 Park Plaza, Suite 5170
Boston, MA 02116

**RE: AICUM's Written Comments on the Amended Standards for
the Protection of Personal Information 201 CMR 17.00**

Dear Undersecretary Crane:

On behalf of the Association of Independent Colleges & Universities in Massachusetts (AICUM) and its 59 member institutions of higher education, we would like to thank you for providing this opportunity to offer written comments on the amended regulations intended to protect the personal information of Massachusetts residents. AICUM supports the underlying principles and goals of the regulations, and the private colleges and universities in Massachusetts have been and will continue to be committed to protecting the personal information of its students, employees and alumni.

AICUM represents the interests of 59 independent colleges and universities throughout Massachusetts, the 250,000 students who attend those institutions and the nearly 100,000 employees who work at those institutions. Our members include large nationally renowned research universities, smaller, highly regarded liberal arts colleges, religiously affiliated institutions, and colleges with special missions focused on business or music or allied health services.

The regulations, however, and particularly the deadlines for complying with the regulations, impose burdens that are virtually impossible for these institutions to meet. For the reasons stated below, AICUM would respectfully request that Governor Patrick and the Office of Consumer Affairs and Business Regulations (OCABR) provide a 90-day period for businesses, industries and the non-profit community to comment on the regulations, re-issue a new set of standards by May 1, 2009 and then allow a two-year period to implement and comply with the new rules.

Cost

The regulations impose a substantial unfunded mandate on colleges and universities. These institutions will incur significant incremental costs as a result of having to purchase new, albeit unproven, software and technology. They also will be required to reallocate existing staff and scarce resources to comply with these regulations.

This unfunded mandate comes at a particularly difficult time for colleges and universities. The ongoing financial crisis has significantly reduced the value of most endowments, restricted other revenue streams, and required schools to direct more money to financial aid to help students –

and their families – complete their education. Many institutions have instituted both budgetary and hiring freezes. Add to this the additional funds that colleges and universities must now expend to comply with new reporting requirements and mandates imposed on them under HEA Reauthorization, FERPA and the FTC “*red flag*” rules. Complying with these regulations will impose a significant new and unanticipated cost at a time when it is most difficult to absorb into an institution’s operating budget.

3rd-Party Verification

The 3rd-party certification provisions included in the regulations are unduly complex, requiring extensive resources and due diligence to certify compliance. Most colleges and universities have hundreds – perhaps thousands – of contracts with outside vendors, a significant portion of which relate to data and documents that contain personal information. Many of these contracts have been in place for years and already contain a variety of provisions designed to protect confidential information, including personal information. To the extent that these pre-existing contract provisions do not meet the requirements contained in the regulations the contracts will have to be renegotiated. This is a task that certainly will take more time than currently contemplated under the regulations.

Obtaining assurances from 3rd-party vendors is a massive undertaking. And doing so before January 1, 2010 will be virtually impossible for AICUM member institutions, particularly for smaller institutions with lean and already over-burdened staffs (IT, legal and procurement). It makes little, if any sense, to enact regulations with the knowledge that such a wide range of institutions and businesses cannot meet the deadlines imposed.

Contract provisions designed to protect personal information have proved effective, and requiring such contract terms in all future transactions involving the personal information of Massachusetts residents would sufficiently safeguard the rights and interests of the citizens of the Commonwealth. Such a requirement would also place the responsibility, and any potential liability for a data breach, on the party that is in the best position to ensure the protection of personal information – namely the business or institution initiating the transaction with an outside 3rd-party vendor. If that 3rd-party vendor then enters into a subsequent transaction with a different vendor the 3rd-party vendor would be charged with requiring contract provisions aimed at safeguarding the personal information. This solution provides certainty by imposing responsibility and potential liability on the party seeking to share the personal information as part of separate, discrete transactions. The regulatory scheme imposed by these regulations puts colleges and universities in the impossible situation of ensuring compliance by vendors 2 or 3 transactions down the line from the original transaction. And vendors outside of Massachusetts are unlikely to know and understand the requirements of these regulations. This is an impossible burden to satisfy, a burden that would impose significant costs on Massachusetts colleges and universities and place them at a competitive disadvantage with colleges and universities in other states.

Inventory

Colleges and universities have a huge volume of records that conceivably come within the scope of these regulations, and this information is widely distributed across several departments. These institutions maintain records for applicants, students (educational and health records), employees, donors, and alumni. It has been – and continues to be – a huge undertaking simply to coordinate where all of these records are stored, identify which department has control of the records, and determine how a more centralized approach to storing and protecting the records can best be achieved. Working groups from each department must be convened, a formal project must be established with key goals addressed sequentially before procedures can be developed, refined and

implemented. In short, this process will consume a lot of time and resources if it is to be done correctly.

Reconciling these new standards with the manner in which existing records have been maintained and stored will take a significant amount of time and resources as well. And designing, testing and implementing a system that will meet all of the requirements of the regulations cannot even begin until an institution completes the inventory required by the regulations. Again, this is a huge undertaking that will require time. Getting it "right" would better serve the underlying public policy than getting it done by some arbitrary deadline.

The current regulations require that "every comprehensive information security system" shall limit the amount of personal information collected. By the nature of their mission, however, colleges and universities can do little to further limit the amount of personal information they must collect. Many, if not all, colleges already have implemented campus ID numbers that are different from Social Security numbers. Moreover, the regulations would require colleges and universities to treat existing "old" records differently from any records that are created on a going-forward basis. College applications, financial aid forms, student records, health records, employment records, and alumni records are all integral parts of the operation of these institutions. In fact, running one of the larger research universities is the equivalent of operating a small city. Colleges and universities can do little, if anything, to further limit the records they must collect to effectively pursue their mission, and requiring colleges and universities to comply with these regulations within such a short deadline sets a goal that is virtually impossible to meet.

It would seem that a more meaningful and cost-effective approach would be to have businesses and non-profit institutions undertake a risk assessment of their record-keeping system and then allow the results of the assessment to identify where resources should be focused. Such an approach would serve the underlying public policy without causing an unnecessary waste of scarce resources.

Encryption

The sweeping mandate of the "encryption requirement" goes beyond the legislative intent of the underlying legislation because the Legislature did not intend to make encryption mandatory. Moreover, the encryption provision would require colleges and universities to invest in software and technology that is complex, costly, and time-consuming, which is particularly onerous for institutions with lean and already over-burdened IT staff because the task of evaluating, acquiring, implementing and supporting encryption will fall squarely on IT.

Evaluating and implementing encryption solutions are complex undertakings, and there is no single technical solution that effectively handles laptops and other portable devices. The diverse systems that currently exist are often not mutually interoperable, and such systems are not widely used by businesses, organizations and individuals in Massachusetts. The challenges of deploying data encryption are highlighted in a recent report from the United States Government Accountability Office entitled *Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, But Work Remains*. Back in 2006, federal agencies were directed to encrypt data. As of a year ago, only 30% of the data was encrypted, and, in some cases where the devices were believed to be encrypted, there were configuration issues or other reasons that resulted in lack of encryption. Mandatory encryption is the wrong solution at the wrong time. The fact that the Commonwealth and its subdivisions will not be required to encrypt or accept encrypted data under these regulations is telling. Requiring colleges and universities that are dealing with unprecedented worldwide financial conditions to test, acquire, and implement encryption hardware and software (that may be obsolete within a short period of time) and pay for related services will only ensure that there is less money for an institution to devote to need-based financial aid, curriculum and student support services, etc.

Since the goal of the Massachusetts regulations is to reduce the risk of data loss that may lead to identity theft, it would seem preferable to implement a carefully designed and sustainable solution, and not force colleges and universities to rush into buying a product which may or may not be effective simply to check off a compliance box.

The need for clarification and education calls for additional time

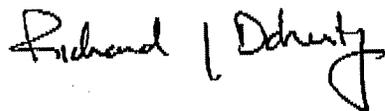
Many colleges and universities use a "point card" system that essentially allows a student to use his/her Student ID card as a declining balance card to make purchases on campus. A student deposits money into an account and then uses his/her ID card to redeem "points" in exchange for books, food, and other goods and services at various locations both on and off campus. Some colleges and universities have received conflicting advice and legal interpretations as to whether such "point cards" are subject to these regulations. Additional time to comment on a new set of regulations would provide an answer to this and similar questions and allow for a more concise and better understood standard.

Analogous Situations

A quick look at several analogous situations will illustrate the need for additional time to comply with these regulations. First, as has been widely broadcast, the United States is currently undergoing a conversion to digital TV. Despite a lead time of more than 4 years to prepare for and educate people about this conversion, President-elect Obama is urging Congress to delay the deadline in order to give people more time to navigate the transition. Second, when colleges and universities had to respond to directives related to Environmental Health and Safety Regulations the process required the dedication of resources over many years. The training phase alone took 18 to 24 months to complete. Third, organizations initially were given a year to comply with the FTC's "Red Flag Rules", but when it became apparent that the rules had a broader impact than originally anticipated, many organizations were given an additional 6 months to comply with rules that had little IT impact. The standards being imposed on businesses and non-profit organizations in Massachusetts were released to the public less than 4 months ago, so asking them to comply with even the extended deadlines is simply unrealistic.

The independent colleges and universities that make up AICUM are committed to protecting the personal information of their students, employees and alumni. AICUM applauds the efforts of Governor Patrick and OCABR in pursuing this important public policy, but we believe that certain provisions of the regulations, coupled with a wholly unrealistic time-frame for compliance, constitute an unfunded mandate that most likely cannot be achieved under current deadlines. We stand ready to work with the Administration and OCABR to create a regulatory scheme that will advance the goal of protecting the personal information of the citizens of Massachusetts without imposing unreasonable burdens and unreachable timetables on the business and non-profit communities.

Very truly yours,



Richard Doherty,
President

Statement of the American Insurance Association

210 CMR 17.00

*Standards for the Protection of Personal Information of
Residents of the Commonwealth*

**Before the Office of Consumer Affairs and Business
Regulation**

January 16, 2009

**John P. Murphy
American Insurance Association
One Walnut Street
Boston, MA 02108
(617) 305-4152**

Thank you for the opportunity to offer comments on 201 CMR 17.00 *Standards for the Protection of Personal Information of Residents of the Commonwealth*. The American Insurance Association (“AIA”) is a national trade association for property and casualty insurance companies with over 350 member companies. AIA members write over \$3.3 billion of premium in Massachusetts and over \$124 billion nationwide. Our carriers include some of the most recognizable brands in America as well as niche players. All of them are committed to protecting the personal information which comes into their possession. AIA appreciates the opportunity to share our members concerns over the regulations proposed by OCABR.

These regulations present both substantive and practical concerns. The original effective date of January 1, 2009—just 3 months after the final regulation was approved—was simply not realistic. Even if companies could ignore every other information technology project on their plates and focus exclusively on implementing this regulation, time would not be sufficient. While AIA greatly appreciates OCABR’s decision to delay implementation for a few months, this “breathing room” will not cure the substantive problems with the regulation or afford companies enough time to fully implement its directives. Many of the requirements of the regulation are unprecedented, extending beyond the identity theft prevention measures enacted in other states. As most of our companies do business in other states, this poses particular hardships and costs.

AIA strongly encourages OCABR to indefinitely delay implementation of the regulation for so that all affected entities can raise concerns and receive guidance from OCABR and the Attorney General, where appropriate. New Jersey’s Department of Consumer Affairs has been grappling with its own version of identity theft regulations. After proposing a regulation in April of 2007, the state withdrew its proposal in response to the comments it received. In December of 2008, after receiving input from affected parties and further reflection, it developed and presented a new draft regulation and solicited further comments. AIA respectfully suggests that Massachusetts undertake a similar approach to vetting this proposal and that when OCABR is ready to adopt the regulation, it provide for a phase-in implementation period.

The regulation seeks to implement the provisions of M.G.L. c. 93H¹ with respect to standards for the protection of personal information of Massachusetts residents.

¹ MGL. c. 93H §2(a) reads: Section 2. (a) 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 personal 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. The objectives of the regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer. The regulations shall take into account the person's size, scope and type of business, the amount of resources available to such person, the amount of stored data, and the need for security and confidentiality of both consumer and employee information.

Unfortunately, rather than providing greater context for what constitutes compliance with the law, this regulation narrows the scope of business options and adds new hurdles for implementation of the legislative intent.

While the delay in the effective date of the regulation relieves some of the immediate pressure on companies, AIA does not want to see these regulations go into effect "as is" when the new effective date arrives. The additional time allows for finding solutions for some of the new challenges, but it does not address some of the fundamental roadblocks and areas where further clarification is needed. These issues include:

- (1) encryption;
- (2) data mapping or data inventory;
- (3) monitoring;
- (4) safeguards consistent with other state or federal regulations; and
- (5) vendor contracting issues.

Before discussing specific concerns in these areas, it is helpful to walk through a balanced approach to protecting data.

AIA believes data security safeguards must follow risk assessments and be appropriate to the size and complexity of the business and the nature and scope of its activities. AIA's approach is consistent with the enabling legislation which states:

"The regulations shall take into account the person's size, scope and type of business, the amount of resources available to such person, the amount of stored data, and the need for security and confidentiality of both consumer and employee information." M.G.L. c. 93H §2(a).

This legislative directive cautions against rigidity and "one size fits all" regulations in favor of allowing businesses flexibility in their protection of personal information.

Identity theft prevention and safeguarding personal information is a consumer protection effort in everyone's best interest. In addition to the individuals who are victimized and angered by ID theft, security breaches can negatively impact a company's brand and consumer loyalty or erode a citizen's confidence in its government when it is involved in a breach. To properly address the concerns and interests of all stakeholders, a reasonable balance needs to guide policy decisions with respect to data security.

Today, budgets are tight and money allocated to those responsible for data security is finite. Requirements should focus on determining where vulnerabilities are the greatest within a company and then on addressing those vulnerabilities. A risk assessment approach to identifying problems and finding solutions is common in business and government and it is fiscally responsible to shareholders, customers and taxpayers. Finding and addressing true privacy risks is a matter of getting the most bang for the data security buck. As drafted, this regulation seems to paint all aspects of security as equally important. They are not.

The most important thing for business to do is to determine where the real risks to personal information are with respect to the kinds of information it has and how such information is transmitted. Next, it needs to secure the data from a top-down approach working first from the highest priority. For those companies that do everything internally, their focus will likely be on the security of data storage and assuring that there are correct controls over access to that data. For those companies that outsource activities dealing with personal information, they need to consider whether that vendor has appropriate security measures in place.

Businesses need a certain amount of flexibility in order to use resources on the most crucial aspects of a company's data security program. The regulation favors rigid rules rather than allowing companies the necessary flexibility to fashion a data security program tailored to its business and the data in its possession. These concepts particularly guide the rationale behind AIA's comments relating to data mapping and encryption.

1. The encryption requirements are too rigid and were not mandated by the enabling legislation. The regulation requires encryption in every instance instead of just those in which the most non-public personal information is exchanged. This approach will have severe negative, unintended consequences. (See Sec. 17.04.)

The encryption provisions raise significant issues since there is no standard way to encrypt emails that go outside a company's network to third parties. Given the size and scope of insurer operations and information at present, there is no consistent platform for sharing an encryption key with an individual consistent with these standards and allow them to read an email. Insurers interact with hundreds of thousands of third parties – doctors, lawyers, claimants, policyholders, hospitals, etc.. There are some third parties with whom insurers communicate fairly regularly, but there are many, many others with whom they deal infrequently. Some interactions may occur only once or may relate to only one claimant. Encryption would not be feasible with these small volume situations. It would slow down the ability to share information and claims could not be handled as quickly. Furthermore, many people prefer to communicate via email and a movement back to paper would be frustrating and counterproductive for the customer.

This is a perfect example of the need for a risk analysis. Other cost-effective approaches may be preferable to encryption. For example, the use of "strong" or "complex" passwords can be effective data safeguards in many contexts. Rather than mandating encryption in all situations, the regulation needs to allow flexibility so that appropriate safeguards can be tailored to the business's unique situation.

Businesses should assess the party with whom they are sharing information as well as the type of data at issue. For regular vendors or a third party administrator, the business may choose to set up a secure pipeline (like a VPN) to transmit encrypted data to and from that entity, which can only be accessed through authentication.

This kind of end-to-end system would not, however, be appropriate for individuals. Developing an alternative for individuals (e.g., a web-based solution) would be extremely expensive to get up and running. One insurer reports that in addition to the start-up

expenses, maintaining such a system would cost over \$750,000 annually. This is an enormous on-going outlay without as much security protection as the bigger (and more manageable) third party business solution.

Requiring encryption for Blackberry and similar devices would not be a wise investment of limited IT resources. Encrypting a Blackberry degrades performance significantly. Further, these devices may be password protected and a business could turn it off ("zap it") immediately when it is lost or stolen or when the individual terminates his or her employment. In such instances, nothing can be accessed. Even if someone were to gain access to a Blackberry (assuming they can get past the password requirement), he or she cannot get to databases but only to that individual's emails. Applying a risk assessment approach, limited resources would be better spent protecting and encrypting laptops with hard drives which can contain spreadsheets and more vulnerable data.

Similarly, the inflexible encryption rules may raise e-discovery concerns. To deal with e-discovery, systems need to allow for searchability and production in the event of actual or threatened litigation. To date, encryption systems with such functionality are costly and impracticable for smaller businesses.

Representative Michael Rodrigues, House Chair of the Committee on Consumer Protection and Professional Licensure and co-author of the enabling legislation, was recently quoted in the *MetroWest Daily News* saying that encryption was not meant to be mandated: "We didn't want to mandate it; we wanted to encourage it," he said. With respect to encryption, this regulation goes beyond the intent of the statute and imposes an unnecessary burden on businesses. The regulation should encourage the use of encryption where appropriate but not require it.

2. Data mapping/inventorying is overly burdensome and the regulations should allow for other ways to address the concern with vulnerability of this data. (See Sec. 17.03(h).)

As drafted, the regulation would require a company to go through all its paper records, as well as its electronic systems to identify where it has personally identifiable information. Going through all kinds of media is an incredibly daunting and almost impossible task. Older companies with legacy systems will have issues because of the sheer volume of data, further complicated if they have undergone mergers or acquisitions with other companies. This is especially the case of financial institutions, like insurers. Also, some companies have numerous locations that serve to magnify the challenges and difficulties of conducting the inventory.

Like the data security concerns discussed above, the scope and detail of the data inventory goes too far. It paints with too broad of a brush, as it regulates down to the minutia. For example, consider how a company might deal with documenting historic use of CDs and paper, especially when thousands of employees work from home. The greatest threat to non-public personal information is through electronic databases or spreadsheets not through individual pieces of paper.

Under a risk assessment review, a company will determine where it has data that is most at risk. The steps taken should be appropriate to the size and complexity of the entity and to the nature and scope of its activities. (See the National Association of Insurance Commissioners (NAIC) Standards for Safeguarding Customer Information Model Regulation.) This kind of activity encourages actively knowing your risks for identity theft and proactively addressing areas where there is the greatest concentration of the most sensitive data. We believe this follows the intent of the law.

3. Monitoring for unauthorized access is costly and should not be necessary if the other prudent steps for securing data are taken. (See Sec. 17.03(j).)

Monitoring for unauthorized access or use may seem reasonable on its face, but if other prudent steps for securing data have been undertaken (*e.g.*, access controls, authentication and encryption for vendor data exchanges) then regular monitoring may not be necessary.

Monitoring is a complex process since trying to isolate the data is difficult. For a countywide insurer, there may be thousands of computer servers with all kinds of data. Further complicating the effort is the fact that some companies have legacy systems in place from the 1960s and 1970s that are not conducive to this kind of activity.

The cost of monitoring can be enormous. One of our member companies received an estimate of \$1.5 million dollars annually for a vendor to periodically scan server logs and automatically flag sets for situations to be reviewed further. This estimate was only for the most critical servers containing the most non-public personal information and was only a periodic scan—not a constant real, time scan. In addition to this significant, on-going outlay, the initial set up costs were estimated to be approximately \$800,000. The regulation calls for regular monitoring in a manner “reasonably calculated” to prevent unauthorized use or access to personal information. It is not clear whether the regulation’s standard would be met even after making this significant financial investment just for the monitoring component of the regulation.

Rather than mandating a monitoring program, the regulations should allow for flexibility and a risk assessment approach so that companies can design programs that protect the data in a sensible and cost-effective manner consistent with the nature of their business.

4. The regulation should include compliance deemer language indicating that compliance with “safeguards for protection of personal information and information of a similar character as set forth in state or federal regulations by which the person who owns, licenses, stores or maintains such information may be regulated.” (See Sec. 17.03, first paragraph.)

The enabling legislation directs that: “Such regulations shall be designed to safeguard the personal 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.” (emphasis added)

Insurers are subject to the data security requirements of Gramm-Leach-Bliley ("GLB") and adherence to those requirements should constitute compliance with Massachusetts law. To do otherwise would subject insurers to over 50 different sets of security systems at an enormous and unnecessary financial cost and would be inconsistent with statutory intent.

AIA recommends that the regulation include compliance deemer language that states that compliance with the federal or state data security regulations for financial institutions as defined by Gramm-Leach-Bliley constitute compliance with the Massachusetts requirements.

5. Businesses need clarification on how to satisfy their contractual requirements with respect to vendors. (See Sec. 17.03(f).) Vendor contracting requirement should only be prospective and not retroactive.

Significant precedent exists for handling third party vendor contract issues on a "going forward" basis, rather than requiring an immediate fix of all existing relationships. AIA strongly believes that the regulation should adopt this approach. (See 17.03(f).)

The focus should be what can reasonably be done. Gramm-Leach-Bliley ("GLB") implementation allowed for grandfathering of vendor agreements. The NAIC's Privacy of Consumer Financial and Health Information Regulation issued post-GLB grandfathered service agreements. It reads:

Two-year grandfathering of service agreements. Until July 1, 2002, a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf satisfies the provisions of Section 15A(1)(b) of this regulation, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before July 1, 2000.

Segmenting new and existing vendor contracts makes sense as a manageable way to handle implementation. It gives business a chance to modify language and processes on a going forward basis without the immediate administrative challenge of identifying the applicable existing vendors, sending them the necessary paperwork and tracking to ensure the documents are ratified.

Insurers need to understand whether they will be deemed to be in compliance when they have an executed agreement with a vendor that mandates the vendor's compliance with applicable state and federal laws and regulations applicable to the products and services they provide.

There should be a safe harbor stating that if a business has a contract requiring a vendor to meet certain standards (for example the ISO standards or other enumerated standards) that a signature on such a contract constitutes certification. In the alternative, if the contract itself will not be automatically deemed compliant with the certification requirement, business needs direction on what specifically the certification should say.

The idea of getting a certification from third party service providers is inconsistent with the established approach for insurers, which requires contracting but not a certification. Consider the real likelihood that some large vendors, potentially including those mandated by state law, may refuse. In these instances, the NAIC Standards for Safeguarding Customer Information Model Regulation Section 8 outlines examples of appropriate data security implementation for overseeing service provider arrangements as including due diligence in selecting the providers. Further it “requires its service providers to implement appropriate measures designed to meet the objectives of this regulation, and, where indicated by the licensee’s risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.” (Emphasis added.) Note that this is not a bright line as it allows for “appropriate steps.”

AIA appreciates the opportunity to air our concerns with 210 CMR 17.00. Our member companies take seriously the obligation to protect the data in their possession and control and hope that Massachusetts will afford companies the flexibility to effectuate that obligation in a reasonable and sensible manner and timeframe.

Friday, January 16, 2009

STATEMENT OF ASSOCIATED INDUSTRIES OF MASSACHUSETTS BEFORE THE OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION REGARDING THE AMENDED REGULATIONS OF 201 CMR 17.00, STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH.

Good afternoon, I am Bradley A. MacDougall, Associate Vice President for Government Affairs for Associated Industries of Massachusetts (AIM), the state's largest nonprofit, nonpartisan association of Massachusetts' employers. AIM and its 6,500 members would like to thank the Office of Consumer Affairs and Business Regulation for extending the general effective date of January 1, 2009 to May 1, 2009. Today, AIM and fellow members of the business community will provide testimony relevant to the amended regulations under 201 CMR 17.00, which provides for the extension of the effective dates by which employers must comply with the new data privacy regulations.

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 and public agencies share 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. However, not "all persons" as regulated under 201 CMR 17.00 are experts nor do all businesses have the resources to hire legal and technology consultants. The business community has already made significant efforts to address the issue of data theft and therefore reasonable public policy must consider that work. The long-term viability of our shared goal, to protect personal data, depends on it.

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.

Today, information and technology is the life-blood of our economy as services strive to meet customer demands in a global market place. Personal data and the protection of this information is a critical and top priority of any business model. Many firms have already invested significant resources and human talent to address the ongoing challenges related to data security. Yet, even those businesses that have made significant investments and time continue to deal with legal and technical challenges.

Now, the mandates included in 201 CMR 17.00 are being forced upon "all persons" and all firms that conduct business in Massachusetts. In sharp contrast, the state of New Jersey is currently in the process of implementing their Data Security laws, which includes a process of more than two years just to promulgate regulations not including actual implementation periods.

Regrettably, the Massachusetts regulations do not provide similar time, clarity or recognition of federal regulations, nor do they recognize the significant technological, legal, operational challenges or the significant investments and human talent that many persons and small firms must now face. Today, "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.

The delay in the general effective date from January 1, 2009 to May 1, 2009 is helpful. However, the underlying problems continue to exist throughout the regulations and the new effective date of May 1, 2009 does not provide sufficient time for public and private entities to become aware of the new regulations, to know what compliance really means and then to locate appropriate resources for the necessary investments required by these regulations. Businesses of all sizes regardless of resources are challenged by the many legal, technical and operational challenges that have been mandated.

AIM believes that the intervening time must be focused on amending these regulations with the direct input of industry experts representing the business, human resources, legal and technical perspectives in collaboration with the Patrick Administration, the Executive Office of Economic Development and Housing, the Office of Consumer Affairs and Business Regulation, the Office of the Attorney General and elected officials.

Since the regulations were finalized on September 22, 2008, AIM has taken several steps to raise awareness, notify and educate our members and the broader business community about the new regulations.¹ AIM has communicated with thousands of Massachusetts businesses and has provided hundreds of Massachusetts employers with education and resources through webinars² and seminars³ 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. Even with this statewide outreach effort an overwhelming number of Massachusetts firms and "persons" are completely unaware of these new regulations. Consistently, businesses would indicate that AIM's communication and education seminar was the first time they were alerted to these new regulations. It is clear that a greater public outreach effort by the administration is necessary in combination with greater time for businesses to implement them.

The following comments reflect some of the questions and feedback from AIM's members:

Awareness and understanding: Most employers are completely 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

¹ Over the past year AIM has communicated to our 7,000 members and the general public through op-eds, quotes in major new publications, in addition to presentation before major trade and industry groups.

² AIM provided four webinars

³ AIM provided six education seminars in 2008 on 201 CMR 17.00 on November 10, Taunton ; November 18, Worcester; December 2, Andover; December 12, Boston; December 15, Chicopee and Pittsfield.

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.

First exposure and training: Consistently, we learned that AIM's communication was their first and that AIM's training represented their first in depth exposure to the law, regulations and the tools needed to assess their data security needs. AIM urges the administration to engage in a greater public outreach effort.

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, 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. Further, 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 written 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.⁴ 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 an evolving and complex discipline – data security. All companies cannot be 100% secure all of the time. There are over a half a billion people with internet access and any of them can pose a danger. Technology, employee training and security practices are continuously evolving. While

⁴ There are at least 44 other states that currently have their own unique Identity Theft or Data Security laws.

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 State of Massachusetts if several of the 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 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. Re-issue an entire set of rules by May 1, 2009 with implementation over a two year period (repealing the existing rules). AIM urges the Department to review the enclosed addendum, which highlights various issues and solutions relative to the rules and their implementation.

Therefore, we respectfully 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.

Addendum: Issues and Solutions for 201CMR 17.00

Below is a listing of issues and solutions that AIM urges further examination:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules. Compliance is an essential goal and this process will provide the best opportunity for regulated parties to understand and reach compliance.

Solution: The State of New Jersey is currently in a two year process just to promulgate a “pre-proposal” of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey’s new pre-proposal provides for a comment period until February 13, 2009. Massachusetts regulations provide far less time. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict with or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Solution: The Massachusetts statute requires consistency with federal law and as written these regulations place Massachusetts in an economic disadvantage. Last year Governor Patrick and Attorney General Coakley engaged in a regulatory review process to analyze and eliminate confusing, onerous and duplicative regulations. 201 CMR 17.00 is one of those very regulations, which that project set out to resolve.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary.

Solutions: Only a contract provision requirement should be used. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Creating contractual provisions should be required of the first initiating party providing the personal data to the next third party so that each discrete data sharing event stands on its own. For example, party A would require a contract provision with party B when A shares personal data with B, but if B then shares the same data with another party then B has the obligation to require contractual provisions from the party it shares such data with. Each sharing would be a discrete contractual transaction. Without such discrete requirements, the contract requirement becomes a never ending, complex, costly, and circular mandate virtually without end. For purposes of comparison, the recent New Jersey pre-proposal contains the following provisions with respect to third parties:

3. Review of service provider agreements by:

- i. Exercising appropriate due diligence in selecting service providers;
- ii. Requiring service providers to implement appropriate measures designed to meet the objectives of this sub-chapter; and
- iii. Taking appropriate steps to confirm that its service providers have satisfied these obligations, when indicated by the risk assessment of the business or public entity; and

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute.

Solutions: A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology. Mandating a specific technique or technology undermines innovation and freezes in place old approaches. A single technology provides an easier target for theft than using a principle or result standard that invites innovative approaches, effective technologies, and flexibility to match circumstances. Inviting innovation by not locking in a single approach ensures that data holders will use up to date software, a concept required under the regulations, and will closely monitor systems.

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated.

Solutions: A better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. Risk analysis reveals strong and weak points of systems, identifies exactly where resources need to be focused to really protect data, and charts accountability. The risk assessment approach would be similar to what is required in other federal and state contexts.

Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations

Solutions: Personal data is an integral part of important global transactions today – in both the public and private sectors. Such data is used for important business, government and personal reasons. The scope of data held and time held are unconnected to breaches provided systems are vibrant and comprehensive – which is exactly what the statute requires subject to severe penalties (as well as destruction of the holder's reputation). Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy.

Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches.

Solutions: Unless the recipient public agency is held to the same standards and requirements as the private sector, the purpose of the statute is frustrated and rendered meaningless. Failure of

the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose.

Below is a listing of issues and solutions related to specific sections of the regulations:

- **Scope of Encryption (17.01 (a) & 17.04 (3)):** As defined encryption is ambiguous and current technological solutions do not provide a universally accepted standard for encrypting data. The legislature did not intend to mandate encryption. As described in testimony by experts, encryption technology is not easily deployable and many private and public sectors will experience significant communication and interoperability malfunctions. The regulations and the nature of technology will force companies to encrypt all data. Personal data is clearly defined in section 17.01 (a) as "the safeguarding of personal information contained in both paper and electronic records" and is further defined in section 17.02. However, section 17.04(3) describes the scope of encryption to include "encryption of all data to be transmitted wirelessly." The requirement that entities must encrypt personal information that will travel across public networks will entail considerable time and money. Encryption is not a standard software for brand new computers. Therefore, new and older system alike will need installation of new software. Again, experts have indicated in their experience that many systems as young as 3 years old have performance problems once encryption software is installed. Can the department guarantee that computers older than 3 years old will have no problems when leaders in the technology field have had a very different experience? Encryption is one of multiple tools for the protection of personal data, however the regulations pick technology "winners and loser", which may be quickly outdated. Further, it provides hackers with a roadmap for attacking all computers. As written, the rules force companies to make an immediate investment on technology and services that are complex and highly specialized. Additionally, the definition of encryption in the regulation remains a concern for many in that it differs from the standard definition in many other states. AIM advocates that encryption should be removed as a mandated rule and that the rules reflect a reasonable approach toward effective tools for protecting data. Further, the rules should reflect
- **Company Size (Section 17.03):** The regulations do not include specific language or guidance for compliance criteria that differentiates a small, midsize or large company as required by paragraph a, section 2 of chapter 93H. For many companies the inventorying process will take months if not years to complete. Individual divisions within a company, consultants and auditors will need to work together to ensure compliance with this requirement. This requirement alone will be very costly and time consuming. One must also keep in mind that data stores and systems are continually growing and evolving from day to day. The inventory would be dated the moment it is completed and would have to be continuously updated imposing significant additional costs on a perpetual basis. AIM advocates that the rules reflect a risk analysis assessment, which will allow businesses with greater flexibility to deal with the constant changes and challenges with protecting data based on the size of the company and resources available as well as a determination of need for the level of security based on the nature of the company's business.

- Federal Standards (Section 17.03):** The regulatory framework goes beyond the requirements of current federal and industry standards causing significant challenges for compliance. These new regulations represent greater compliance implications including a more rigorous security management program that includes written security policies for any company, regardless of size, conducting business in Massachusetts. The regulations also require a separate and unique data breach notifications. Currently 44 states have unique data security laws and firms must operate nationally and globally. Companies now face a challenge to integrate complicated and costly technological solutions to segregate and protect the personal information of anyone from Massachusetts apart from all other personal information from residents of other states. Additionally, any company's employees would need explicit authorization to access any personal information of a Massachusetts resident. AIM advocates that firms currently regulated under federal standards should be considered to be in compliance.
- Contracts & Third Party Vendors (Section 17.03 (f)):** This is one of the most troubling aspects of the regulations. Companies desire to work with reputable businesses and make significant efforts to work vendors that protect data. As proposed, all companies must first obtain a written statement from a third party vendor prior to the vendor's access to any personal information. A third party vendor's written statement must detail that all data will be protected as prescribed under the law and regulations of 93H. The regulations do not explicitly mention if an electronic statement is sufficient for compliance. Even with the extension of the deadline, many firms outside of Massachusetts or globally are completely unaware of these rules. Regulated parties under these rules will face a significant economic disadvantage, because many vendors have already chosen, or will choose not to amend a contract. Therefore, many firms will have to go through a costly and time consuming vendor recertification process. Amending contracts is not simple and cannot be done quickly as the timeline within the rules indicate. This process will take a considerable amount of time. Further, many companies are both vendors and suppliers, which has already caused significant challenges with contract renegotiations. Another concern for business is the issue of retroactive vendor certification on existing contracts. There is a real problem between opening existing contracts vs. just adding it to new contracts and renewals contracts. Boilerplate contract language does not suffice; contracts between individual parties will need to be amended because such provisions are not self-activating. The process is not simple, and any firm that sends their vendor(s) a written certification could expect that their contracts need to be reformed. This adds considerable time and opens up further negotiations on other terms within the contract. For example, not all contracts have provisions that provide latitude for a firm to quickly amend a contract and further a vendor or customer may have provisions will allow a customer to cancel or be released from the contract based on a change in law. AIM advocates that this regulation could halt business operations within the Massachusetts economy. Companies under Federal compliance demands were granted at least 2 years to complete this task.. A contract provision requirements should be used only. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed.

- **Identifying paper, electronic and other records (17.03 (h)):** As proposed, records must be identified to determine which records contain personal information. For most companies, this process will take months if not years to complete. Individual divisions within a company, consultants and auditors will need to work together to ensure compliance with this requirement. This requirement alone will be very costly and time consuming. One must also keep in mind that data stores and systems are continually growing and evolving from day to day. The inventory would be dated the moment it is completed and would have to be continuously updated imposing significant additional costs on a perpetual basis. AIM advocates the rules be amended to include a risk analysis assessment, which will allow businesses with greater flexibility to deal with the constant changes and challenges with protecting data based on the size of the company and resources available as well as a determination of need for the level of security based on the nature of the company's business.
- **Scope of the term "Public Network" (Section 17.04 (3)):** The term is ambiguous and might be challenging for companies that rely on multiple networks for internal and mobile communications. As defined, this term could include all networks for any data regardless of where the data is stored or accessed. Additionally, the definition of encryption in the regulation remains a concern for many in that it differs from the standard definition in many other states. The requirement that entities must encrypt personal information that will travel across public networks will entail considerable time and money. New systems could be encrypted in many situations at additional cost, but for systems purchased even just a few years ago it would be difficult, expensive and often impossible to add encryption capabilities retroactively. This type of immediate investment presents an unfair burden to businesses. AIM advocates that clarification of the term public network should be defined as the networks utilized to transfer personal data as defined by section 17.01 (a) and 17.02.
- **Reasonably Up-to-Date (17.04 (6-7)):** The regulations call on businesses to have the most reasonable and up-to-date software protection. However, the regulations prescribe that all computer software must be programmed to receive the most current security updates on a regular basis. This is a problem for small to midsize companies, where security software and hardware are costly. It appears that all data regardless of the information's sensitivity must be protected through the purchase of costly hardware and software. Further, technology experts have observed that in some instances computer hard drives that are three (3) years old have become inoperable once encryption software was installed. Therefore, this regulation would force business to purchase brand new equipment. AIM advocates that companies would benefit from a risk analysis model.

----- Original Message -----

From: bounce@bounce.votervoice.net <bounce@bounce.votervoice.net>

To: Secretary Daniel O'Connell <Daniel.O'Connell@state.ma.us>

Sent: Tue Jan 13 12:39:01 2009

Subject: Change Mass. Data Regulations

Secretary O'Connell:

As an employer in Pepperell, MA with 26 employees, I am very concerned about the mandates currently included in 201 CMR 17.00. As written, these regulations set a difficult course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth.

We agree that keeping personal information confidential has and will continue to be a responsibility that employers assume. However, in most cases the information that is defined as "personal information" is required by an employer only to fulfill government requirements. The one exception being financial account number required for direct payroll deposits.

I urge my elected officials to review the statement given by AIM dated November 19, 2008. The statement clearly defines the issues, concerns and obstacles businesses will have in implementing 201 CMR 17.00.

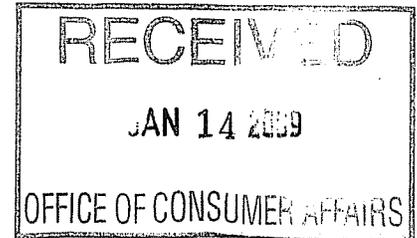
I also ask that my elected officials recognize that AIM represents me and my company while I am busy trying desperately to save jobs. I have been informed that some elected officials do not recognize AIM as a representative of the business community. I would ask these elected officials give AIM the same weight they give union officials. I am sure no elected official would ever say that a union does not represent its members.

Lastly, I take issue that all government agencies are exempt from this standard. Is that because steps have already been taken by the numerous government agencies that hold this personal information or that it would be difficult for them to comply?

Sincerely,

Albert Polmonari
CEO
Astron, Inc.
21 Lomar Park
Pepperell, MA 01463

BANAS & FICKERT INSURANCE AGENCY
63 MAIN ST., EASTHAMPTON, MA 01027
413-527-2700 - FAX 413-527-0900
E-mail: mikebanasins@onceanddone.com
Website: www.banasinsurance.com



January 13, 2009

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

Top Priority: Protect Personal Information through Stakeholder Analysis

Dear Undersecretary Crane and General Counsel Murray:

As an (**employer or employee**) with (**X number**) of employees, I am very concerned, about the mandates currently included in 201 CMR 17.00. As written, these regulations set a perilous course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth. I urge the Patrick's Administration Patrick's Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 with the Department, Attorney General, regulated community and elected officials, to re-issue an entire set of rules by May 1, 2009 with implementation of the rules over a two year period.

As a business owner or employee the protection of personal information for residents of the Commonwealth is a top priority. The delay in the effective date is helpful, as a practical matter, it is unreasonable to believe that my firm has a fair opportunity to reach full compliance. As currently written, 201 CMR 17.00 goes beyond the legislature's intent and mandates specific technologies, creates redundant and confusing rules and does not hold public agencies to the same standards of the private sector. In many instances the regulatory mandates are not technically or economically feasible for public or private agencies regardless of size or available resources. Further, the regulations do not envision the national and global business relationships that the Massachusetts economy depends on.

The implications of 201 CMR 17.00 will have a negative impact on "all persons" and all firms that conduct business in Massachusetts. The promulgation and implementation of these specific regulations are in sharp contrast with other states and especially other Massachusetts state agencies that routinely engage in collaborative discussions with the regulated communities. The state of New Jersey recognized the need for a vigorous

stakeholder analysis. Currently, the State of New Jersey is currently in a two year process just to promulgate a "pre-proposal" of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey's new pre-proposal provides for a comment period until February 13, 2009. Regrettably, the Massachusetts regulations do not provide similar time, clarity, recognition of federal regulations nor do they recognize the significant technological, legal, operational challenges or the significant investments and human talent that many persons and small firms must now face.

The following is a partial list of the issues and solutions that the business community has identified:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules to achieve the ultimate goal of compliance. The regulations should be implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Otherwise the contract and written certification requirement becomes a never ending, complex, costly, and circular mandate virtually without end.

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute. A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology.

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated. A

better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. The risk assessment approach would be similar to what is required in other federal and state contexts.

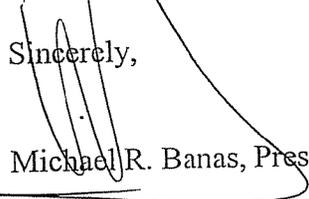
Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations. Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy

Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose

Under these rules "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 to "all persons" or firms, regardless of readily available resources.

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. Thank you for considering the long-term implications of these regulations and their direct impact on my business and the Massachusetts economy.

Sincerely,


Michael R. Banas, President

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

Dear Mr. Murray:

I am writing concerning the timing of regulations proposed by the Department of Consumer Affairs and Business Regulation (OCABR) to implement M.G.L. c. 93H as codified in 201 CMR 17.00.

Specifically, I am concerned about the January 1, 2010 deadline for portable devices other than laptops as delineated in 201 CMR 17.04(5) in relation to 201 CMR 17.02 and .03's definition of a "person" and current IRS regulations.

As a Massachusetts resident, I am certainly in favor of protecting the personal information of Massachusetts residents. Your office is already familiar with the difficulties in obtaining adequate encryption technology, however, for portable devices such as PDAs and cell phones, or else you would not have extended the deadline to January 1, 2010.

Perhaps you are not aware, however, of how IRS regulations are impacting the handling of these devices by various institutions within the Commonwealth. I attach at the end of this letter an opinion Boston College received from Price Waterhouse Coopers vis-à-vis cell phones and an opinion on the same from Grant Thornton, another public accounting firm. In the past, the university purchased cell phones for the use of employees where there was a clear business need, and accepted that in today's society, the employees might make personal calls on these devices from time to time as well.

The IRS, however, has clarified that such devices are defined as "listed property" and that as a result, any use for non-business calls must be individually documented, on a per-call basis. Because of the IRS's position, Boston College and many other institutions have moved to a model where cell phones and "smart" phones/PDAs are no longer purchased by the university. Instead, employees with a need are given an allowance in the payroll system to offset their cost in personally purchasing whatever cell phone brand and plan they desire. This stance allows the university to avoid the wrath of the IRS, and dispenses with the need for employees to keep individual logs of each personal cell phone call they make so they can then reimburse the university. It also, however, creates a situation where the university has significantly diminished control over what cell phone or smart phone employees use, and the software (including encryption) deployed on the phone.

A phone purchased in this manner, to make the IRS happy, is not property of the university in any way. Employees can visit their nearest electronics or cellular retailer and purchase whatever device they wish. The overwhelming majority of

these devices are consumer-grade, and, as a result, do not have encryption capabilities.

This brings me to responsibility. 201 CMR 17.02 defines a “person” as “a natural person, corporation...or other legal entity...” 201 CMR 17.03 states that “Every person that...stores or maintains personal information about a resident of the Commonwealth shall develop, implement, maintain and monitor a comprehensive, written information security program...”

If an individual employee of Boston College buys a cell phone or smart phone with his or her own funds, I submit that the individual, and not Boston College, is the owner of that phone. If the individual then stores “personal information” as defined by M.G.L. 93H on the phone, I submit that the individual is a “natural person” under 201 CMR 17.02’s definition. The logical conclusion, then, is that the individual employee is personally responsible for the information on the phone that he or she owns, and not Boston College.

As 201 CMR 17.00 is presently cast, one might argue that the employees are “third-party service providers” under 17.03(f). But such providers are not formally defined in the regulation, and it flies in the face of logic to suggest that an employee is a third-party service provider. Irrespective, under 17.03 each individual BC employee who purchases their own cell phone and ends up with personal information of a resident of the Commonwealth on said phone, by definition must have a comprehensive written information security program related to his or her personal cell phone. Even if the “third-party” provider logic above held, which as I noted I do not think is the case, Boston College would then under 17.03(f) have to obtain a statement from each employee with a cell phone who might have access to personal information that said employee was in compliance with 201 CMR 17.00, which again means each employee having an information security program related to his or her personal cell phone.

I suggest that the paucity of encryption software available on consumer cell phones and PDAs, in combination with the IRS “listed property” regulation, which forces institutions without sophisticated call recordkeeping systems to allow employees to buy their own portable phones or smartphones has created an unintentional consequence. Specifically, the OCABR has created the consequence in the current draft of 201 CMR 17.00 of forcing numerous individual residents of the Commonwealth to comply in full with the regulation. I further suggest that, given this difficulty, the OCABR extend the deadline for other portable devices past the January 1, 2010 date until such time as the regulation can be crafted around this issue, or manufacturers of consumer portable phones can place standardized encryption on them, much like air bags are now standard on cars, in order to protect the residents of our Commonwealth properly without exposing potentially large numbers of them to maintaining written information security programs for their portable phones.

Boston College appreciates the opportunity to comment on the proposed regulations and the Department's efforts to implement the Legislature's intent. I would be happy to provide further explanation on any of the comments in this letter or to have discussions with the Department about any portion of 201 CMR 17.00. The documents from Price Waterhouse Coopers and Grant Thornton follow.

Thank you for your time and consideration.

David Escalante
Director of Computer Policy & Security
Boston College

Listed Property - Substantiation Rules
August 11, 2006

General Rules on Substantiation of Business Use:

- Cell phones (or similar telecommunications equipment) are defined as listed property (I.R.C. §280F(d)(4)(A)(v))
- When listed property is provided to an employee by an employer:
 - a.) An employee may not exclude from gross income as working condition fringe any amount of the value of the availability of listed property provided by an employer to the employee unless the employee substantiates the amount of the exclusion (Treas. Reg. §1.274-5T(e)(1)(i))
 - b.) The employer can substantiate its *business use* through evidence that shows that the listed property was used by the employee in the employer's trade or business and, if any employee used the property for personal purposes, the employer includes an appropriate amount in the employee's income (Treas. Reg. §1.274-5T(e)(2)(i)(A))
 - c.) Relying on the Employee's record:
 - The employer may rely on adequate records maintained by the employee:
 - a. Unless the employer know or has reason to know that the records are not accurate

- b. The employer must retain a copy of the adequate records maintained by the employee

OR

- The employer can rely on a statement submitted by the employee that provides sufficient information to allow the employer to determine the business use of the property:
 - a. Employer can rely on employee statement unless the employer knows or has reason to know that the statement is not based on adequate records
 - b. If the employer relies on the employee's statement, the employer must retain only a copy of the statement - the employee must retain a copy of the adequate records

(Treas. Reg. §1.274-5T(e)(2)(ii))

General Rules on Substantiation of Business Use (continued):

- To prove the business use of listed property the amount, the time, and the business purpose must be substantiated as follows:
 - a.) The amount of:
 - Expenditure - each separate expenditure with respect to an item of listed property
 - Use - the amount of each business use based on appropriate measure (i.e. minutes)
 - b.) Time - date of use
 - c.) Business purpose - the business purpose for use

Treas. Reg. §1.274-5T(b)(6)

- Adequate records - an account book, diary, log, statement of expense, or similar record must be prepared or maintained in such a manner that each recording of an element of a use is made at or near the time of the use (Treas. Reg. § 1.274-5T(c)(2)(ii)):
 - a.) At or near the time of use - a log, record, etc. submitted by an employee to the employer in the "regular course of good business practice"
 - b.) A written statement is generally required to constitute an adequate record of business purpose
 - c.) Listed property - substantiation of business use - the record must contain sufficient information as to each element of every business use (Treas. Reg. §1.274-5T(c)(2)(ii)(C))

- Sampling - use of listed property - substantiation by other sufficient evidence:
 - a.) Records can be maintained for a portion of the year, and
 - b.) Periods for which an adequate record is maintained must be representative of the use for the year
- (Treas. Reg. §1.274-5T(c)(3)(ii))
- Listed property is not eligible for the no-cost additional fringe benefit (Treas. Reg. §1.132-5T(c)(1))

Grant Thornton LLP Not for Profit Tax Alert, March 4, 2008

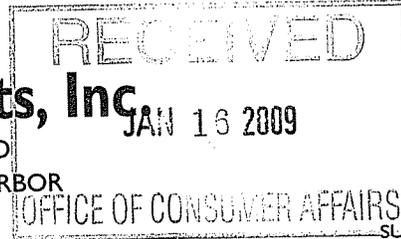
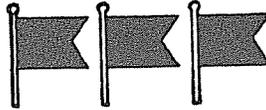
Relief may be on the way for organizations that provide cell phones to employees Representative Sam Johnson of Texas and six co-sponsors introduced legislation on Feb. 14, 2008, that would amend the Internal Revenue Code of 1986 to remove cell phones from "listed property" under section 280F. If enacted in its current form, the MOBILE Cell Phone Act would mean that personal use of employee paid cell phones and cell phone service would no longer be subject to the onerous record-keeping requirements under the listed property rules. This would help eliminate the reporting and intermediate sanctions risks associated with this common but problematic employee benefit.

Current law can result in automatic excess benefits Under the current tax law, cell phones (and similar telecommunication devices such as the Blackberry®, Treo, etc.) are considered listed property. The working condition fringe benefit rules apply to cell phones and other listed property only when the item is used for business purposes. As a result, the business use versus personal use of these items is required to be tracked contemporaneously by employees, in order to properly exclude the value of the use of the item from the employee's gross income. Generally, a business log or diary indicating business use and prepared contemporaneously is required in order to disprove personal use, and thus prevent compensation treatment for listed property provided as an employee benefit. Otherwise, the entire benefit is normally includable as wage income. While all employers face an income tax withholding and payroll tax risk, the additional problem for Section 501(c)(3) and Section 501(c)(4) organizations is that if the value of the personal use of telecommunication devices is not properly documented as compensation for employees who are provided these items, intermediate sanctions may apply if the individuals are considered disqualified persons under IRC 4958. The IRS has applied these laws to hold that using employer equipment (and reimbursements for purported but not properly recorded business use) can result in wage income, which, if unreported on Form W-2 or other tax form, can result in an automatic excess benefit subject to intermediate sanctions. This presents a serious risk for a seemingly minor and ubiquitous fringe benefit.

REPAIRS/REFITTING
STORAGE
TRAVELIFT/CRANE SERVICE
HELIX MOORINGS
WESTERBEKE ENGINES
YANMAR ENGINES
UNIVERSAL ENGINES
VOLVO ENGINES

Burr Brothers Boats, Inc.

FULL SERVICE YACHT YARD
AT THE HEAD OF SIPPICAN HARBOR



MERCURY
EVINRUDE
HONDA
YAMAHA
SUNFISH / LASER
DINGHIES / INFLATABLES
CHARTS & HARDWARE
SEALAND-VACUFLUSH

309 Front Street Marion, MA 02738 • Telephone 508-748-0541 • Fax 508-748-0963
E-mail: burrbros@burrbros.com Web: www.burrbros.com

January 15, 2009

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

Dear Mr. Crane and Mr. Murray,

We take good care of our customers private information. And, we have never had an incident where information was lost. The new regulations are extremely expensive and small companies are already struggling to get along.

Sincerely,

A handwritten signature in cursive script that reads "Ellen Hull for Today's Burr".

Carleton Burr, Jr.

CB,Jr.:eh

January 16, 2009

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

Top Priority: Protect Personal Information through Stakeholder Analysis

Dear Undersecretary Crane:

As leaders in business, the protection of personal information is a top priority and we write on behalf of a very broad range of businesses and industries that serve Massachusetts residents to express our deep concerns regarding many of the requirements of 201 CMR 17.00. While the delay in the effective date is helpful, it is unreasonable to believe, as a practical matter, that businesses or government agencies will have a fair opportunity to reach full compliance with these regulations as currently written. The requirements imposed by 201 CMR 17.00 set a difficult course for public and private entities, hindering our ability to invest and protect jobs in the Commonwealth. The Business Coalition urges the Patrick Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 so that the Department, Attorney General, regulated community and elected officials, can re-issue an entire set of rules by May 1, 2009, allowing for a two year period within which to implement the revised regulations.

As public policy matter, the business community supports laws and efforts aimed at protecting the personal information for residents of the Commonwealth. In fact, the business community demands that the successful implementation of regulations is necessary to protect personal information in the private and public sectors and to prevent further economic distress caused by the loss of personal data. However, regulations within 201 CMR 17.00 set a perilous course for already strained individuals, families, businesses and state agencies that depend upon the success and growth of the Massachusetts economy.

As currently written, 201 CMR 17.00 goes beyond the Legislature's intent through highly prescriptive mandates. For example, the Legislature never intended to make encryption mandatory. In many instances the regulatory mandates are not technically or economically feasible. Further, the regulations do not envision the national and global business relationships that Massachusetts firms depend on.

The implications of 201 CMR 17.00 will have a negative impact on "all persons" and all firms that conduct business in Massachusetts. In sharp contrast, the state of New Jersey is currently in the process of implementing their data security laws, which includes a process of more than two years just to promulgate regulations not including actual implementation periods.

Regrettably, the Massachusetts regulations do not provide similar time, clarity, recognition of federal regulations nor do they recognize the significant technological, legal, operational

challenges or the significant investments and human talent that many persons and small firms must now face. Today, "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 to "all persons" or firms, regardless of readily available resources. The following is a partial list of the issues and solutions that the business community has identified:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules. Compliance is an essential goal and this process will provide the best opportunity for regulated parties to understand and reach compliance.

Solution: The State of New Jersey is currently in a two year process just to promulgate a "pre-proposal" of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey's new pre-proposal provides for a comment period until February 13, 2009. Massachusetts regulations provide far less time. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict with or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Solution: The Massachusetts statute requires consistency with federal law and as written these regulations place Massachusetts in an economic disadvantage. Last year Governor Patrick and Attorney General Coakley engaged in a regulatory review process to analyze and eliminate confusing, onerous and duplicative regulations. 201 CMR 17.00 is one of those very regulations, which that project set out to resolve.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary.

Solutions: A contract provision requirements should be used only. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Creating contractual provisions should be required of the first initiating party providing the personal data to the next third party so that each discrete data sharing event stands on its own. For example, party A would require a contract provision with party B when A shares personal data with B, but if B then shares the same data with another party then B has the obligation to require contractual provisions from the party it shares such data with. Each sharing would be a discrete contractual transaction. Without such discrete requirements, the contract requirement becomes a never ending, complex, costly, and circular

mandate virtually without end. For purposes of comparison, the recent New Jersey pre-proposal contains the following provisions with respect to third parties:

3. Review of service provider agreements by:
 - i. Exercising appropriate due diligence in selecting service providers;
 - ii. Requiring service providers to implement appropriate measures designed to meet the objectives of this sub-chapter; and
 - iii. Taking appropriate steps to confirm that its service providers have satisfied these obligations, when indicated by the risk assessment of the business or public entity; and

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute.

Solutions: A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology. Mandating a specific technique or technology undermines innovation and creativity, and it freezes in place old approaches. A single technology provides an easier target for theft than using a principle or result standard that invites innovative approaches, effective technologies, and flexibility to match circumstances. Inviting innovation by not locking in a single approach ensures that data holders will use up to date software, a concept required under the regulations, and will closely monitor systems.

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated.

Solutions: A better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. Risk analysis reveals strong and weak points of systems, identifies exactly where resources need to be focused to really protect data, and charts accountability. The risk assessment approach would be similar to what is required in other federal and state contexts.

Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations

Solutions: Personal data is an integral part of important global transactions today – in both the public and private sectors. Such data is used for important business, government and personal reasons. The scope of data held and time held are unconnected to breaches provided systems are vibrant and comprehensive – which is exactly what the statute requires subject to severe penalties (as well as destruction of the holder’s reputation). Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy.

Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches.

Solutions: Unless the recipient public agency is held to the same standards and requirements as the private sector, the purpose of the statute is frustrated and rendered meaningless. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose.

Data security is not simple, no one person in a firm can provide the expertise and no one technological solution will provide security. The Business Coalition urges the Patrick Administration to provide an opportunity for greater stakeholder analysis with the Department, Attorney General, regulated community and elected officials. We must get this right – cost effective data privacy rules that comply with the statute, set standards, recognize existing programs, and invite innovation.

These comments represent but a few of the concerns the business community has with the Standards. Others include, but are not limited to: the Standards' encryption requirement that, for many businesses, will require abandoning existing systems and investing in completely new (and likely expensive) hardware and software that can accommodate encryption; the requirement to only provide electronic information in an encrypted form, which is impractical unless the recipient of such information – including the Commonwealth and its sister states are able and willing to accept encrypted information (which is not the case today); requiring the revision of all contracts with third-party vendors to ensure they include provisions expressly addressing data security; inconsistency with other state/Federal data security requirements; limitations on the use and maintenance of information; the costs associated with implementation; and the overly aggressive compliance date for implementing the Standards.

Therefore, 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 administration to allow for this process, to re-issue an entire set of rules by May 1, 2009 with implementation of the rules over a two year period. Thank you for considering the long-term implications of these regulations for the protection of personal information of Massachusetts residents and the Massachusetts economy.

We appreciate your consideration of these concerns and strongly urge your assistance in working together with us on a solution, as New Jersey was able to accomplish by the Government and private sector working in tandem, to the above concerns that is in the best interest of the Commonwealth, its citizenry, and the business community.

Sincerely,

AeA
Affiliated Chambers of Commerce of Greater Springfield
American Insurance Association
American Rental Association of Massachusetts Inc.
American Staffing Association
Andover Country Club, Inc

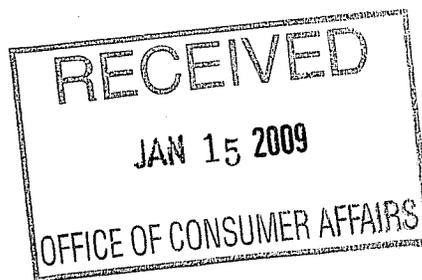
AOL
Associated Industries of Massachusetts
Association of Independent Colleges and Universities in Massachusetts
AT&T
Avedis Zildjian Co.
Cambridge Chamber of Commerce
CitiGroup
Comcast
Consumer Data Industry Association
Costco Wholesale Corp.
CSW, Inc.
CTIA—The Wireless Coalition
First Data
Google
Greater Boston Chamber of Commerce
Greater Gardner Chamber of Commerce
Internet Alliance
Investment Companies Institute
Liberty Mutual
Life Insurance Association of Massachusetts
Massachusetts Marine Trades Association
Massachusetts Staffing Association
Massachusetts Association of Health Underwriters
Massachusetts Association of Insurance Agents
Massachusetts Bankers Association
Massachusetts Biotechnology Council
Massachusetts Business Roundtable
Massachusetts Council of Human Service Providers, Inc.
Massachusetts Food Association
Massachusetts High Technology Council & Defense Technology Institute
Massachusetts Hospital Association
Massachusetts Insurance Federation, Inc.
Massachusetts Mortgage Bankers Association
Massachusetts Package Store Association
Massachusetts Retail Lumber Dealers Association
Massachusetts Senior Care Association
Massachusetts Society of Certified Public Accountants
Massachusetts Technology Leadership Council
Mental Health and Substance Abuse Corporations of Massachusetts, Inc.
Metro South Chamber of Commerce
MetroWest Chamber of Commerce
Microsoft
Monster.com
National Federation of Independent Business/Massachusetts
National Retail Federation
New England Financial Services Association

North Central Massachusetts Chamber of Commerce
North Suburban Chamber of Commerce
Property Casualty Insurers Association of America
Reed Elsevier
Retail Industry Leaders Association
Retailers Association of Massachusetts
Rocky's Hardware
Securities Industry and Financial Markets Association
South Shore Chamber of Commerce
State Privacy and Security Coalition
Target Corporation
TechNet
The Gap
T-Mobile
Verizon
Walmart Stores, Inc.
Waltham West Suburban Chamber of Commerce
Worcester Regional Chambers of Commerce

Cc: Governor Deval Patrick
Lt. Governor Timothy Murray
Attorney General Martha Coakley
Speaker Salvatore DiMasi
President Therese Murray
Chairman Michael Morrissey
Chairman Michael Rodrigues
Secretary Daniel O'Connell
Gregory Bialeki, Undersecretary

January 15, 2009

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



Top Priority: Protect Personal Information through Stakeholder Analysis

Dear Undersecretary Crane:

As leaders in business, the protection of personal information is a top priority and we write on behalf of a very broad range of businesses and industries that serve Massachusetts residents to express our deep concerns regarding many of the requirements of 201 CMR 17.00. While the delay in the effective date is helpful, it is unreasonable to believe, as a practical matter, that businesses or government agencies will have a fair opportunity to reach full compliance with these regulations as currently written. The requirements imposed by 201 CMR 17.00 set a difficult course for public and private entities, hindering our ability to invest and protect jobs in the Commonwealth. The Business Coalition urges the Patrick Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 so that the Department, Attorney General, regulated community and elected officials, can re-issue an entire set of rules by May 1, 2009, allowing for a two year period within which to implement the revised regulations.

As public policy matter, the business community supports laws and efforts aimed at protecting the personal information for residents of the Commonwealth. In fact, the business community demands that the successful implementation of regulations is necessary to protect personal information in the private and public sectors and to prevent further economic distress caused by the loss of personal data. However, regulations within 201 CMR 17.00 set a perilous course for already strained individuals, families, businesses and state agencies that depend upon the success and growth of the Massachusetts economy.

As currently written, 201 CMR 17.00 goes beyond the Legislature's intent through highly prescriptive mandates. For example, the Legislature never intended to make encryption mandatory. In many instances the regulatory mandates are not technically or economically feasible. Further, the regulations do not envision the national and global business relationships that Massachusetts firms depend on.

The implications of 201 CMR 17.00 will have a negative impact on "all persons" and all firms that conduct business in Massachusetts. In sharp contrast, the state of New Jersey is currently in the process of implementing their data security laws, which includes a process of more than two years just to promulgate regulations not including actual implementation periods.

Regrettably, the Massachusetts regulations do not provide similar time, clarity, recognition of federal regulations nor do they recognize the significant technological, legal, operational

challenges or the significant investments and human talent that many persons and small firms must now face. Today, “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 to “all persons” or firms, regardless of readily available resources. The following is a partial list of the issues and solutions that the business community has identified:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules. Compliance is an essential goal and this process will provide the best opportunity for regulated parties to understand and reach compliance.

Solution: The State of New Jersey is currently in a two year process just to promulgate a “pre-proposal” of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey’s new pre-proposal provides for a comment period until February 13, 2009. Massachusetts regulations provide far less time. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict with or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Solution: The Massachusetts statute requires consistency with federal law and as written these regulations place Massachusetts in an economic disadvantage. Last year Governor Patrick and Attorney General Coakley engaged in a regulatory review process to analyze and eliminate confusing, onerous and duplicative regulations. 201 CMR 17.00 is one of those very regulations, which that project set out to resolve.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary.

Solutions: A contract provision requirements should be used only. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Creating contractual provisions should be required of the first initiating party providing the personal data to the next third party so that each discrete data sharing event stands on its own. For example, party A would require a contract provision with party B when A shares personal data with B, but if B then shares the same data with another party then B has the obligation to require contractual provisions from the party it shares such data with. Each sharing would be a discrete contractual transaction. Without such discrete requirements, the contract requirement becomes a never ending, complex, costly, and circular

mandate virtually without end. For purposes of comparison, the recent New Jersey pre-proposal contains the following provisions with respect to third parties:

3. Review of service provider agreements by:

- i. Exercising appropriate due diligence in selecting service providers;
- ii. Requiring service providers to implement appropriate measures designed to meet the objectives of this sub-chapter; and
- iii. Taking appropriate steps to confirm that its service providers have satisfied these obligations, when indicated by the risk assessment of the business or public entity; and

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute.

Solutions: A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology. Mandating a specific technique or technology undermines innovation and creativity, and it freezes in place old approaches. A single technology provides an easier target for theft than using a principle or result standard that invites innovative approaches, effective technologies, and flexibility to match circumstances. Inviting innovation by not locking in a single approach ensures that data holders will use up to date software, a concept required under the regulations, and will closely monitor systems.

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated.

Solutions: A better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. Risk analysis reveals strong and weak points of systems, identifies exactly where resources need to be focused to really protect data, and charts accountability. The risk assessment approach would be similar to what is required in other federal and state contexts.

Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations

Solutions: Personal data is an integral part of important global transactions today – in both the public and private sectors. Such data is used for important business, government and personal reasons. The scope of data held and time held are unconnected to breaches provided systems are vibrant and comprehensive – which is exactly what the statute requires subject to severe penalties (as well as destruction of the holder’s reputation). Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy.

Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches.

Solutions: Unless the recipient public agency is held to the same standards and requirements as the private sector, the purpose of the statute is frustrated and rendered meaningless. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose.

Data security is not simple, no one person in a firm can provide the expertise and no one technological solution will provide security. The Business Coalition urges the Patrick Administration to provide an opportunity for greater stakeholder analysis with the Department, Attorney General, regulated community and elected officials. We must get this right – cost effective data privacy rules that comply with the statute, set standards, recognize existing programs, and invite innovation.

These comments represent but a few of the concerns the business community has with the Standards. Others include, but are not limited to: the Standards' encryption requirement that, for many businesses, will require abandoning existing systems and investing in completely new (and likely expensive) hardware and software that can accommodate encryption; the requirement to only provide electronic information in an encrypted form, which is impractical unless the recipient of such information – including the Commonwealth and its sister states are able and willing to accept encrypted information (which is not the case today); requiring the revision of all contracts with third-party vendors to ensure they include provisions expressly addressing data security; inconsistency with other state/Federal data security requirements; limitations on the use and maintenance of information; the costs associated with implementation; and the overly aggressive compliance date for implementing the Standards.

Therefore, 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 administration to allow for this process, to re-issue an entire set of rules by May 1, 2009 with implementation of the rules over a two year period. Thank you for considering the long-term implications of these regulations for the protection of personal information of Massachusetts residents and the Massachusetts economy.

We appreciate your consideration of these concerns and strongly urge your assistance in working together with us on a solution, as New Jersey was able to accomplish by the Government and private sector working in tandem, to the above concerns that is in the best interest of the Commonwealth, its citizenry, and the business community.

Sincerely,

AeA
Affiliated Chambers of Commerce of Greater Springfield
American Insurance Association
American Rental Association of Massachusetts Inc.
American Staffing Association
Andover Country Club, Inc

AOL
Associated Industries of Massachusetts
Association of Independent Colleges and Universities in Massachusetts
AT&T
Avedis Zildjian Co.
Cambridge Chamber of Commerce
CitiGroup
Comcast
Consumer Data Industry Association
Costco Wholesale Corp.
CSW, Inc.
CTIA—The Wireless Coalition
First Data
Google
Greater Boston Chamber of Commerce
Greater Gardner Chamber of Commerce
Internet Alliance
Investment Companies Institute
Liberty Mutual
Life Insurance Association of Massachusetts
Massachusetts Marine Trades Association
Massachusetts Staffing Association
Massachusetts Association of Health Underwriters
Massachusetts Association of Insurance Agents
Massachusetts Bankers Association
Massachusetts Biotechnology Council
Massachusetts Business Roundtable
Massachusetts Council of Human Service Providers, Inc.
Massachusetts Food Association
Massachusetts High Technology Council & Defense Technology Institute
Massachusetts Hospital Association
Massachusetts Insurance Federation, Inc.
Massachusetts Mortgage Bankers Association
Massachusetts Package Store Association
Massachusetts Retail Lumber Dealers Association
Massachusetts Senior Care Association
Massachusetts Society of Certified Public Accountants
Massachusetts Technology Leadership Council
Mental Health and Substance Abuse Corporations of Massachusetts, Inc.
Metro South Chamber of Commerce
MetroWest Chamber of Commerce
Microsoft
Monster.com
National Federation of Independent Business/Massachusetts
National Retail Federation
New England Financial Services Association

North Central Massachusetts Chamber of Commerce
North Suburban Chamber of Commerce
Property Casualty Insurers Association of America
Reed Elsevier
Retail Industry Leaders Association
Retailers Association of Massachusetts
Rocky's Hardware
Securities Industry and Financial Markets Association
South Shore Chamber of Commerce
State Privacy and Security Coalition
Target Corporation
TechNet
The Gap
T-Mobile
Verizon
Walmart Stores, Inc.
Waltham West Suburban Chamber of Commerce
Worcester Regional Chambers of Commerce

Cc: Governor Deval Patrick
Lt. Governor Timothy Murray
Attorney General Martha Coakley
Speaker Salvatore DiMasi
President Therese Murray
Chairman Michael Morrissey
Chairman Michael Rodrigues
Secretary Daniel O'Connell
Gregory Bialeki, Undersecretary

From: bounce@bounce.votervoice.net on behalf of Willa Giordano
[wgiordano@centralmassmachine.com]
Sent: Tuesday, January 13, 2009 12:34 PM
To: General Counsel David Murray
Subject: Change Mass. Data Regulations

General Counsel Murray:

Our facility, Central Mass. Machine, Inc., has been machining very large parts in Holyoke for over 100 years. From Massachusetts, our parts (up to 30,000 lbs) are shipped world-wide for power plants, for defense and for industry. As both controller and human resource manager for our 37 employees, I am very concerned about the mandates currently included in 201 CMR 17.00. As written, these regulations set a difficult course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth.

We make all efforts to comply with existing privacy, HIPAA and data security regulations. We need to protect both the business's data and the personal information of our employees. But the new CMR is so vague, ambiguous and convoluted that it defies logic. We need clear guidelines, no more burdensome than Federal regulations, to effectively manage this issue. Please reconsider implementation until these goals met. Thank you for your attention.

Sincerely,

Willa Giordano
Controller
Central Mass. Machine, Inc.
529 S East St
Holyoke, MA 01040



Chisholm insurance agency, inc.

January 15, 2009

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

Top Priority: Protect Personal Information through Stakeholder Analysis

Dear Mr. Murray:

As an employer with 5 employees, I am very concerned, about the mandates currently included in 201 CMR 17.00. As written, these regulations set a perilous course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth. I urge the Patrick's Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 with the Department, Attorney General, regulated community and elected officials, to re-issue an entire set of rules by May 1, 2009 with implementation of the rules over a two year period.

As a business owner, the protection of personal information for residents of the Commonwealth is a top priority. The delay in the effective date is helpful, as a practical matter, it is unreasonable to believe that my firm has a fair opportunity to reach full compliance. As currently written, 201 CMR 17.00 goes beyond the legislature's intent and mandates specific technologies, creates redundant and confusing rules and does not hold public agencies to the same standards of the private sector. In many instances the regulatory mandates are not technically or economically feasible for public or private agencies regardless of size or available resources. Further, the regulations do not envision the national and global business relationships that the Massachusetts economy depends on.

The implications of 201 CMR 17.00 will have a negative impact on "all persons" and all firms that conduct business in Massachusetts. The promulgation and implementation of these specific regulations are in sharp contrast with other states and especially other Massachusetts state agencies that routinely engage in collaborative discussions with the regulated communities. The state of New Jersey recognized the need for a vigorous stakeholder analysis. Currently, the State of New Jersey is in a two year process just to promulgate a "pre-proposal" of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey's new pre-proposal provides for a comment period until February 13, 2009. Regrettably, the Massachusetts regulations do not provide similar time, clarity, recognition of federal

regulations nor do they recognize the significant technological, legal, operational challenges or the significant investments and human talent that many persons and small firms must now face.

The following is a partial list of the issues and solutions that the business community has identified:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules to achieve the ultimate goal of compliance. The regulations should be implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Otherwise the contract and written certification requirement becomes a never ending, complex, costly, and circular mandate virtually without end.

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute. A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology.

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated. A better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. The risk assessment approach would be similar to what is required in other federal and state contexts.

Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations. Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy

Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose

Under these rules "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 to "all persons" or firms, regardless of readily available resources.

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. Thank you for considering the long-term implications of these regulations and their direct impact on my business and the Massachusetts economy.

Sincerely,



Thomas B. Chisholm
President

Cc: Senator Michael W. Morrissey, Chairman
Committee on Consumer Protection & Professional Licensure

Rep. Michael J. Rodrigues, Chairman
Committee on Consumer Protection & Professional Licensure

The City of Revere Massachusetts



City Hall

281 BROADWAY
REVERE, MA 02151
(781) 289-3288 RESIDENCE
(781) 289-5099 FAX

Office of the City Council

Daniel Rizzo

Councilor-at-Large

Governor Deval Patrick
Massachusetts State House
Office of the Governor
Room 360
Boston, MA 02133

Secretary Daniel O'Connell
Executive Office of Housing & Economic Development
One Ashburton Place, Room 2101
Boston, MA 02108

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

CC: Senator Anthony Galluccio, Senator Anthony Petruccelli, Senator Michael W. Morrissey, Chairman
Committee on Consumer Protection & Professional Licensure, Rep. Michael J. Rodrigues, Chairman
Committee on Consumer Protection & Professional Licensure, Representative Robert DeLeo, Representative Kathi
Reinstein, Mayor Thomas G. Ambrosino, Revere Chamber of Commerce

Top Priority: Protect Personal Information through Stakeholder Analysis

Dear Governor Patrick, Secretary O'Connell and Undersecretary Crane:

As current President of the Revere City Council and as an employer with 6 employees, I am very concerned, about the mandates currently included in 201 CMR 17.00.

As written, these regulations set a perilous course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth. I urge the Patrick's Administration Patrick's Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 with the Department, Attorney General, regulated community and elected officials, to re-issue an entire set of rules by May 1, 2009 with implementation of the rules over a two year period.

As a business owner, the protection of personal information for residents of the Commonwealth is a top priority. The delay in the effective date is helpful, as a practical matter, it is unreasonable to believe that my firm has a fair opportunity to reach full compliance.

As currently written, 201 CMR 17.00 goes beyond the legislature's intent and mandates specific technologies, creates redundant and confusing rules and does not hold public agencies to the same standards of the private sector. In many instances the regulatory mandates are not technically or economically feasible for public or private agencies regardless of size or available resources. Further, the regulations do not envision the national and global business relationships that the Massachusetts economy depends on.

The implications of 201 CMR 17.00 will have a negative impact on “all persons” and all firms that conduct business in Massachusetts. The promulgation and implementation of these specific regulations are in sharp contrast with other states and especially other Massachusetts state agencies that routinely engage in collaborative discussions with the regulated communities. The state of New Jersey recognized the need for a vigorous stakeholder analysis. Currently, the State of New Jersey is currently in a two year process just to promulgate a “pre-proposal” of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey’s new pre-proposal provides for a comment period until February 13, 2009. Regrettably, the Massachusetts regulations do not provide similar time, clarity, recognition of federal regulations nor do they recognize the significant technological, legal, operational challenges or the significant investments and human talent that many persons and small firms must now face.

The following is a partial list of the issues and solutions that should be addressed:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules to achieve the ultimate goal of compliance. The regulations should be implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Otherwise the contract and written certification requirement becomes a never ending, complex, costly, and circular mandate virtually without end.

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute. A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology.

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated. A better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. The risk assessment approach would be similar to what is required in other federal and state contexts.

Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations. Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy

Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches. We know this in dealing with our constituents on a daily basis. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute’s purpose

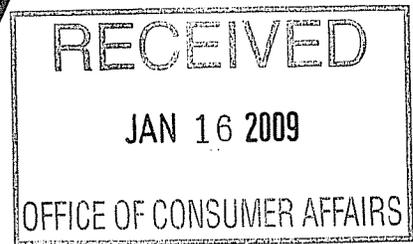
Under these rules “all persons” and firms regulated cannot achieve 100% compliance because these regulations ignore the fact that many of the technological, legal and operational requirements are not readily available to “all persons” or firms, regardless of readily available resources.

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. Thank you for considering the long-term implications of these regulations and their direct impact on my business and the Massachusetts economy.

Sincerely,

Daniel Rizzo
Revere City Council President



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

January 14, 2009

Top Priority: Protect Personal Information through Stakeholder Analysis

Dear Undersecretary Crane:

As an employer with 30 full-time employees, I am very concerned, about the mandates currently included in 201 CMR 17.00. As written, these regulations set a perilous course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth. I urge the Patrick Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 with the Department, Attorney General, regulated community and elected officials, to re-issue an entire set of rules by May 1, 2009 with implementation of the rules over a two year period.

As a business owner, the protection of personal information for residents of the Commonwealth is a top priority. The delay in the effective date is helpful, as a practical matter, it is unreasonable to believe that my firm has a fair opportunity to reach full compliance. As currently written, 201 CMR 17.00 goes beyond the legislature's intent and mandates specific technologies, creates redundant and confusing rules and does not hold public agencies to the same standards of the private sector. In many instances the regulatory mandates are not technically or economically feasible for public or private agencies regardless of size or available resources. Further, the regulations do not envision the national and global business relationships that the Massachusetts economy depends on.

The implications of 201 CMR 17.00 will have a negative impact on "all persons" and all firms that conduct business in Massachusetts. The promulgation and implementation of these specific regulations are in sharp contrast with other states and especially other Massachusetts state agencies that routinely engage in collaborative discussions with the regulated communities. The state of New Jersey recognized the need for a vigorous stakeholder analysis. Currently, the State of New Jersey is currently in a two year process just to promulgate a "pre-proposal" of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey's new pre-proposal provides for a comment period until February 13, 2009. Regrettably, the Massachusetts

226 Causeway Street, Ste 302
Boston, MA 02114-2155
617.723.0700
617.723.7275 Fax

21 McGrath Hwy, Ste 305
Quincy, MA 02169-5351
617.773.8888
617.770.2780 Fax

regulations do not provide similar time, clarity, recognition of federal regulations nor do they recognize the significant technological, legal, operational challenges or the significant investments and human talent that many persons and small firms must now face.

The following is a partial list of the issues and solutions that the business community has identified:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules to achieve the ultimate goal of compliance. The regulations should be implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Otherwise the contract and written certification requirement becomes a never ending, complex, costly, and circular mandate virtually without end.

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute. A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology.

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated. A better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. The risk assessment approach would be similar to what is required in other federal and state contexts.

Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations. Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy

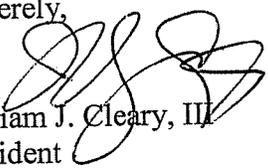


Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose

Under these rules "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 to "all persons" or firms, regardless of readily available resources.

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. Thank you for considering the long-term implications of these regulations and their direct impact on my business and the Massachusetts economy.

Sincerely,



William J. Cleary, III
President
Cleary Insurance, Inc.
226 Causeway Street, Suite 302
Boston, MA 02114-2155





COLLEGE OF THE HOLY CROSS

Timothy F. Mines
General Counsel



January 21, 2009

Secretary Daniel O'Connell
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116

Re: Protect Personal Information through Stakeholder Analysis

Dear Secretary O'Connell:

As an employer with over 800 employees, I am very concerned about the mandates in 201 CMR 17.00. These regulations set a perilous course for this College, the state and our shared goals to invest and protect jobs in the Commonwealth. I urge the Patrick Administration to engage in a rigorous stakeholder analysis and transparent comment process focused on the entire set of regulations within 201 CMR 17.00 with the Department, Attorney General, regulated community, and elected officials with a goal to issue an entirely new set of rules, with implementation over a two year period.

The protection of personal information for residents of the Commonwealth is a top priority for everyone. However, as currently written, 201 CMR 17.00 goes beyond the legislature's intent and mandates specific technologies, creates redundant and confusing rules and does not hold public agencies to the same standards as the private sector. In many instances the regulatory mandates are not technically or economically feasible for public or private agencies regardless of size or available resources. Further, the regulations do not envision the national and global business relationships that the Massachusetts economy depends on.

The current rules will have a negative impact on "all persons" and all firms that conduct business in Massachusetts. The promulgation and implementation history of these specific regulations are in sharp contrast with other states and even other Massachusetts state agencies that routinely engage in extensive and vibrant collaborative discussions with the regulated communities. The state of New Jersey recognized the need for a vigorous stakeholder analysis. Currently, the State of New Jersey is engaged in a two year process just to promulgate a "pre-proposal" for data privacy regulations and that does not include the phase in time for actual compliance. Regrettably, the Massachusetts process for our privacy regulations did not provide similar time, clarity, education, and recognition of federal regulations, nor do the rules recognize

the significant technological, legal, operational challenges, or the significant investments and human talent that many persons and small firms must now face.

The following is a partial list of the issues and solutions that the business community has identified:

Time: Time is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules to achieve the ultimate goal of compliance. The resulting regulations should be implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community.

Consistency: Consistency with existing and soon to be promulgated federal law and the laws of other states is essential, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict other federal and state laws and provide little or no additional substantive protection for Massachusetts consumers, employees and other residents.

Contract provisions and written certifications: The third party contractual obligations and separate certification are duplicative, confusing, and unnecessary. Contractual language requiring third parties holding personal data to protect such information should be used. Otherwise the contract obligations and written certification requirements becomes a never ending, complex, costly, and essentially circular mandate virtually without end.

Mandatory encryption: Encryption of data is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard the Legislature put in the law. A standard for the outcome protecting personal data should be used allowing the regulated community to develop a range of measures for protection, rather than complying with a single command and control technology requirement.

Inventory: The inventory requirement to find every piece of personal data is a complex, costly and counterproductive effort, drawing resources away from more important privacy objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated. A better, more meaningful approach is to undertake a risk analysis of systems identifying the potential for the loss of such data. The risk assessment approach would be similar to what is required in other federal and state contexts.

Information collected and time held: Data collecting and holding requirements are problematic and the regulatory structure does not require such rules. Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy.

Public sector: Massachusetts agencies need to be held to exactly the same standards as the private sector for data privacy. Personal data is regularly shared with public entities and has the potential to be a source of significant data breaches. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose.

In the final analysis, under the existing rules "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 to "all persons" or firms, regardless of available resources.

Data security is not simple, no one person in a firm can provide the expertise, and no single technological solution will work in all situations. We must get this right – cost effective data privacy rules that comply with the statute, set standards, recognize existing programs, and invite innovation. Thank you for considering the long-term implications of these regulations and their direct impact on the College and the Massachusetts economy.

Sincerely,



Timothy F. Mines, Esq.
General Counsel

From: bounce@bounce.votervoice.net on behalf of Ann Lukasik [alukasik@cswwgraphics.com]
Sent: Tuesday, January 13, 2009 12:33 PM
To: General Counsel David Murray
Subject: Change Mass. Data Regulations

General Counsel Murray:

As an employer in the Ludlow, MA with 100 employees, I am very concerned about the mandates currently included in 201 CMR 17.00. As written, these regulations set a difficult course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth.

I feel the upcoming notifications regarding security incidents involving personal information will become as common place, meaningless and as ignored as the privacy statements now are.

The cost to comply will involve hiring a consultant to determine that our computer systems meet the requirements.

In our attempts to comply I have run across our vendors that our not prepared to address this situation.

Also the requirement to inventory all records that contain personal information seems arbitrary, time-consuming and useless.

Please do what you can to reduce the compliance burden to Massachusetts employers who are already struggling to survive in this economy.

Sincerely,

Ann Lukasik
Controller
CSW, Inc.
45 Tyburski Rd
Ludlow, MA 01056

From: djkern@comcast.net
Sent: Wednesday, January 21, 2009 4:54 PM
To: Murray, David (SCA)
Subject: What about protecting Massachusetts' CITIZENS?
Attachments: What about protecting MA residents OCABR.doc

Attention: David A. Murray

What about protecting Massachusetts' CITIZENS?

201 CRM 17.00, Standards for the Protection of Personal Information of Residents of the Commonwealth has already been delayed from January 1, 2009 to May 1, 2009 and January 1, 2010.

Now, as reported by THE ASSOCIATED PRESS on January 17, 2009 in the Worcester Telegram article "New identity theft rules protested" <http://www.telegram.com/article/20090117/NEWS/901170311/-1/NEWS> companies and advocates have asked the Patrick administration in a 1/15/09 letter to

1. reissue new regulations on May 1
2. give them two additional years to comply.

In doing this, how many millions of innocent victims will have their personal and financial lives torn apart; have their medical records compromised; have warrants for their arrest and so much more.

I appreciate that the economy is in shambles. I can also see how the regulations are a challenge in both cost and complexity. But what makes me ill is that

Businesses should be responsible to know that since the nations first disclosure bill CA 1386, (effective July 1, 2003) that privacy issues were being seriously neglected and that breaches were required to be disclosed unless the privacy data had been encrypted. I feel they could have done more and any further delays are unwarranted.

Business hasn't done the right things; they've done the least that they could to slide by!

After almost 5-years of data breach disclosures and daily news reports of problems, business owners, associations and advocates shouldn't be acting as if they are the victims. Claiming that "personal data protection and reporting is too costly and complex" is really unfair to the commonwealth's residents. It would be one thing if the Bay State was the first in the nation with a data protection law but being the 44th state is something else.

Besides, Massachusetts has the great distinction of being the home base of TJX who precipitated the loss of almost 100 million credit card numbers that fueled many serious extended identity theft issues.

We need privacy protection

As a resident, I applaud the effort as Massachusetts residents absolutely need privacy protection and anyone that has been a victim of identity theft knows the absolute frustration that lasts years and never seems to go away. I feel the Federal Trade Commission's finding that 28% of ID theft victims are never able to completely put the facts back prior to being victimized is very accurate .

Because a business was sloppy with the private information of my family members, they have spent hundreds of hours trying to clear their good names, reputations and credit rankings. I can't tell you the number of times they have been put on hold by phone systems, credit bureaus and other institutions.

The time away from their jobs, their family time and continued "proving themselves innocent as the system has declared them guilty" is wrong. The double checking of every bill, statement, medical procedure, calling law enforcement to investigate fraudulent warrants for arrest and the hours spent crying and worrying if this nightmare will ever come to an end is just not right.

It's simply unbelievable what can happen when your life is turned upside down. In fact, one member was denied a loan, another lost a job opportunity.

And they will never know if that criminal is still using their identity at this very moment.

Businesses do not have any problem at all charging the profit margin on the goods and services. Why can't they do the basic, moral thing and do to protect every customer's private data and financial records?

They have asked me to ask our elected officials (Governor Patrick, the Office of Consumer Affairs and Business Regulations (OCABR) and the Attorney General's office (AG) to start protecting them and all Massachusetts citizens.

At the very least, businesses should be forced to

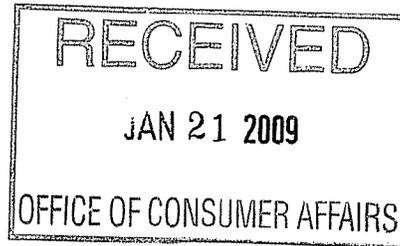
1. Immediately report if data has been compromised.
2. Immediately train their people so that everyone knows how to protect both physical and cyber data
3. Maintain a written policy so that everyone within the company is operating efficiently and is on the same page as to addressing procedures, discussing potential shortcomings and to know how to handle mistakes before they become catastrophic in a systematic manner.

Thank you for this opportunity to express a combination of views.

DJ Kern

California Senate Bill 1386

This bill, operative July 1, 2003, would require a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The bill would permit the notifications required by its provisions to be delayed if a law enforcement agency determines that it would impede a criminal investigation. The bill would require an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data, as specified. The bill would state the intent of the Legislature to preempt all local regulation of the subject matter of the bill. This bill would also make a statement of legislative findings and declarations regarding privacy and financial security.



January 21, 2009

Daniel O'Connell
Secretary of Housing and Economic Development
c/o Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116

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

Dear Secretary O'Connell:

As Chairman and Chief Executive Officer of Eaton Vance Corp., a Massachusetts-based investment management company with over 800 employees in the Commonwealth, I feel it is important to let you know my concerns regarding the recently adopted Standards for the Protection of Personal Information of Residents of the Commonwealth (the "New Privacy Rules"). The New Privacy Rules will put a substantial burden on all firms doing business in the Commonwealth and will have a particularly adverse effect on investment management organizations and the funds they manage.

On November 17, 2008, two Eaton Vance employees along with representatives from seventeen other well-known investment managers in Massachusetts and the Investment Company Institute (the "ICI")¹ met with Messrs. Crane and Murray at the Office of Consumer Affairs and Business Regulation (the "OCABR"), and then Messrs. Conroy, Scafide and Clements of the Office of the Attorney General (the "OAC") to discuss the significant impact of the New Privacy Rules on investment management firms doing business in Massachusetts. During the course of these meetings, the OCABR and the OAC encouraged companies to inform senior leadership in Massachusetts of concerns raised by the New Privacy Rules. Eaton Vance also has been working with the ICI to help educate the OCABR and OAC about the adverse impact of the New Privacy Rules on the investment management industry (including investment advisers, broker-dealers and transfer agents) and, more particularly, mutual funds. Eaton Vance supported Ms. Tamara Salmon, Esq., a senior representative of the ICI, in her testimony before the Joint Committee on Consumer Protection and Professional Licensure on November 19, 2008 and before the OCABR's public hearing on January 16, 2009.

¹ The ICI is the national association of U.S. investment companies, including mutual funds, closed-end funds, exchange-traded funds, and unit investment trusts. The 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 the ICI manage total assets of \$9.86 trillion and serve almost 93 million shareholders.

Current Privacy Protections. Eaton Vance is compelled by regulations and fiduciary principles to protect client information. Eaton Vance and other investment management companies are required to comply with numerous federal and state privacy regulations, which mandate maintaining client privacy and require that privacy breaches be communicated to clients. Regulation S-P, adopted in response to the federal Gramm-Leach-Bliley Act and administered by the U.S. Securities and Exchange Commission, the recently adopted "Red Flag Rule" administered by the Federal Trade Commission, and Massachusetts' existing privacy rules, along with those of other states, have led to the development of robust privacy protections for clients of investment management firms.

While regulatory requirements compel the protection of client information, protecting client information also is inherent in the fiduciary relationship investment management firms have with their clients. Eaton Vance and its service providers, as well as other firms in the investment management industry, have worked diligently to create and maintain a secure environment that ensures the privacy of client data. In preserving the privacy of client data, Eaton Vance employs data encryption and firewall security that benefits from some of the latest technologies. Similar to many other investment management companies, Eaton Vance has a Chief Privacy Officer who is charged with oversight of our privacy policies and procedures. In protecting the privacy of clients, Eaton Vance monitors the use of client information to ensure it is only used for the purpose of providing client services, and stores this information in a manner designed to ensure that it is not lost or misused. In addition, Eaton Vance requires firms to which client information is provided to contractually agree to protect the confidentiality of such information. To ensure the effectiveness of our privacy program, we conduct periodic audits of our compliance with our privacy policies and procedures. Maintaining the privacy of our clients is a significant business priority at Eaton Vance; we have established strong and effective policies and procedures to support this effort.

The New Privacy Rules. Our primary concerns with the New Privacy Rules are as follows:

- *The New Privacy Rules contain requirements that exceed the requirements imposed upon investment management firms by federal regulations.* Section 2(a) of M.G.L. c. 93H, pursuant to which the New Privacy Rules were adopted, requires in part that the OCABR adopt regulations "*consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated.*" (Emphasis added). However, as described below, certain provisions of the New Privacy Rules, such as those mandating written certificates and specific computer systems requirements, are not consistent with federal regulations and create significant new burdens on investment management companies and mutual funds doing business in Massachusetts.

- *The requirements to amend existing contracts and obtain written certificates before providing access to personal information are unduly burdensome.* Investment management firms have extensive relationships with third party service providers. Similarly, mutual funds, which typically do not have employees, rely heavily on third party service providers for their operation.² As required by applicable law, most contracts with investment management firms or mutual funds relating to servicing of client or shareholder accounts contain a provision requiring that client or shareholder information be protected. A similar provision is included in the New Privacy Rules. The New Privacy Rules differ from previous regulations in that they mandate a written certification from each service provider that such provider has a written comprehensive security program that complies with the New Privacy Rules. In order to comply with this requirement, we estimate we may be required to amend over 3,000 contracts with third parties that provide servicing to Eaton Vance and/or the mutual funds that we sponsor.³ This would be a very significant undertaking, involving many hundreds of hours of negotiation and attorney time. For the mutual funds, the high cost of this effort would be borne by fund shareholders. Because some service providers may not otherwise be subject to the New Privacy Rules and therefore may be unwilling to certify that they comply with the New Privacy Rules, or may be unable to comply with the unique provisions of the Rules (such as those relating to encryption), Eaton Vance or a fund may have to terminate service relationships to the detriment of clients or shareholders.

In addition to the burden of complying with the written certification requirement, certain provisions of that requirement are ambiguous. Funds and investment managers frequently receive subpoenas for information from other states and information requests from regulatory bodies asking for client information. For instance, funds and investment managers are often requested by various state entities to provide client data regarding unpaid child support and are subpoenaed by various state or other regulatory entities to furnish client data. Regulatory bodies may be unwilling to provide the written certification required by the New Privacy Rules, which would result in delayed responses to, or non-compliance with, requests from other states.

² Attached hereto is a table prepared by the ICI that details the various relationships between funds and their service providers.

³ The burden associated with a requirement to amend contracts and to require written certifications is apparently recognized in Governor Patrick's Executive Order No. 504, Order Regarding the Security and Confidentiality of Personal Information (the "Order"). Unlike section 17.03(f) of the New Privacy Rules, which would require all businesses to revise all existing contracts with third-parties, under the Order, state agencies are only required to amend contracts entered into after January 1, 2009. None of the other requirements of the Order are subject to a compliance date, presumably in recognition of the difficulties associated with compliance with timeframes such as those under the New Privacy Rules.

- *The specific technical requirements in the New Privacy Rules are overly restrictive.* The New Privacy Rules enumerate specific electronic security provisions that must be employed by companies to safeguard personal information. By mandating the means by which a company must comply with the New Privacy Rules, companies are precluded from developing privacy protection technologies that may better address the privacy concerns associated with their particular business. Moreover, some recipients of data that meet the encryption requirements of the New Privacy Rules may be unable to access encrypted data, including certain agencies of the Commonwealth.
- *The New Privacy Rules create a disincentive to do business in Massachusetts.* It is important to note that most of the service providers with whom Eaton Vance and the funds do business currently are subject to, or are contractually bound to comply with, stringent federal and state privacy regulations. To require these service providers to provide a written certificate of compliance with the New Privacy Rules may serve as a disincentive for such service providers to do business in Massachusetts and/or to service residents of the Commonwealth.

Requested Action. In light of these concerns, we respectfully request that you take action to amend or otherwise revise the New Privacy Rules. Specifically, we request that the New Privacy Rules be amended to provide that they do not apply to entities to the extent such entities are subject to federal privacy regulations, such as Regulation S-P. Alternatively, we would recommend the following:

- That the requirement to obtain written certifications from service providers be eliminated from the New Privacy Rules; and
- That the provisions requiring the use of specific technology and/or specific security provisions in transmitting and storing electronic data be eliminated from the New Privacy Rules.

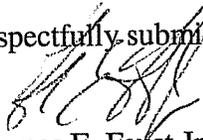
If the foregoing amendments to the New Privacy Rules cannot be implemented before the initial effectiveness date of May 1, 2009, we request that compliance with all provisions of the New Privacy Rules be delayed until not earlier than January 1, 2011 so that the necessary contractual amendments can be negotiated, written certifications can be obtained, and specific technologies can be implemented, or, if needed, service providers who do not agree to the amendments or certificates, or who cannot work with the mandated technologies, can be replaced.

As stated above, client privacy is of the highest concern to Eaton Vance, and we believe it is well guarded under existing regulations. We hope to work with you to ensure the continued safety of client data, while providing our clients with the level of service and cost effectiveness that they require.

Daniel O'Connell
Secretary of Housing and Economic Development
Page 5 of 5

I appreciate your attention to this matter. Please contact me if you would like to discuss further the New Privacy Rules and their impact on investment managers and the funds they sponsor.

Respectfully submitted,



Thomas E. Faust Jr.
Chairman and Chief Executive Officer
Eaton Vance Corp.

Cc: Daniel C. Crane, Undersecretary
Office of Consumer Affairs and Business Regulation

David A. Murray, General Counsel
Office of Consumer Affairs and Business Regulation

The Honorable Deval Patrick, Governor
The Commonwealth of Massachusetts

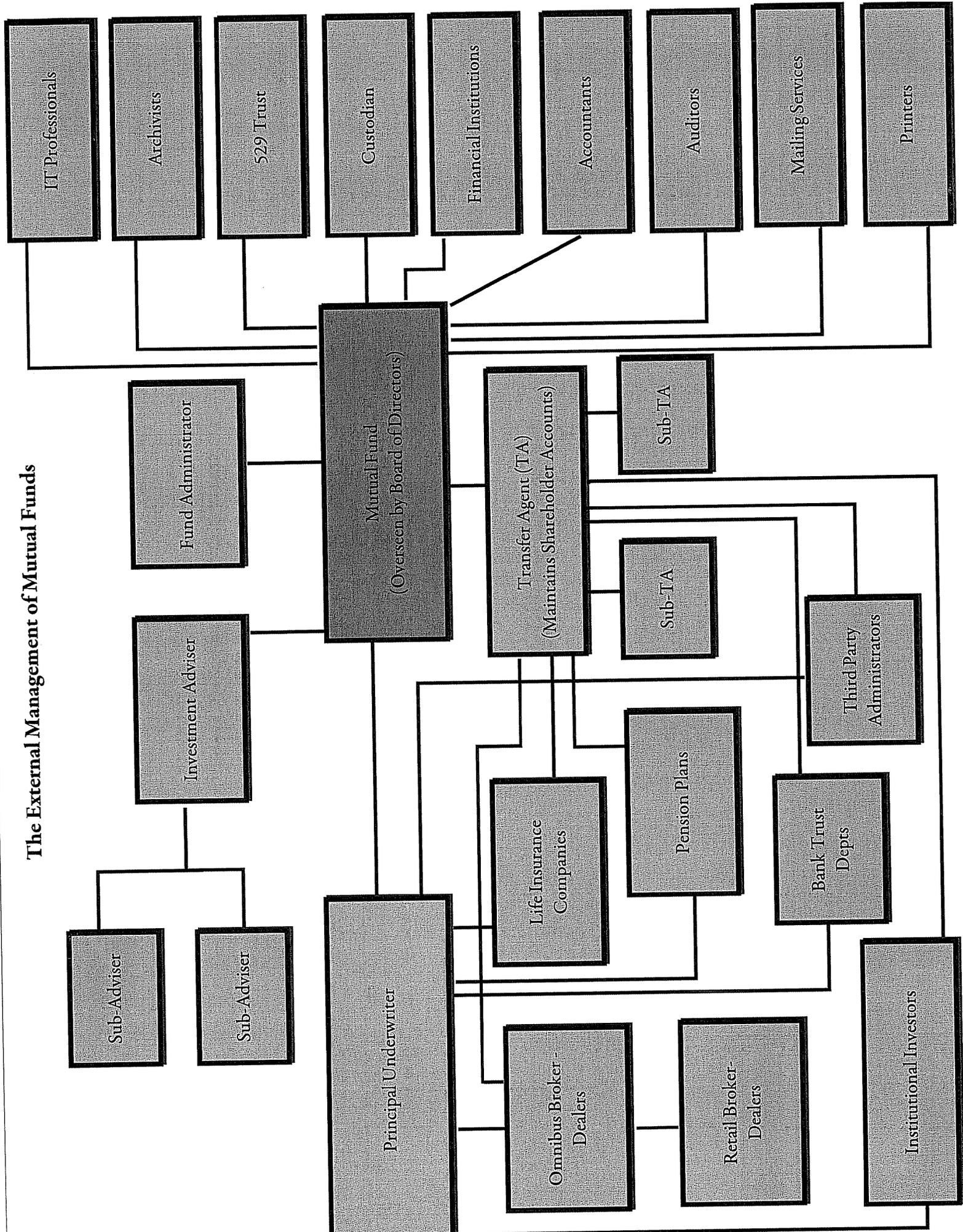
Martha Coakley, Attorney General
The Commonwealth of Massachusetts

Representative Michael J. Rodrigues, Co-Chair
Joint Committee on Consumer Protection and Professional Licensure

Senator Michael W. Morrissey, Co-Chair
Joint Committee on Consumer Protection and Professional Licensure

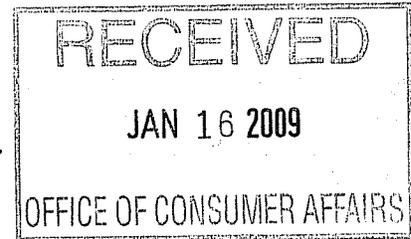
Tamara K. Salmon, Senior Associate Counsel
Investment Company Institute

The External Management of Mutual Funds





42 Industrial Way, Wilmington, MA 01887
www.ebeam.com



January 9, 2009

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

Top Priority: Protect Personal Information through Stakeholder Analysis

Dear Undersecretary Crane:

As leaders in business, the protection of personal information is a top priority, but we express our deep concerns regarding many of the requirements of 201 CMR 17.00 and its affect on small business, in particular to businesses that have minimal exposure to data breach of MA residents. Collaboration with the MA business community is essential to minimize the burden and maximize the success of this type of legislation. Its easier to do it right NOW vs. later!

The requirements imposed by 201 CMR 17.00 set a difficult course for public and private entities, hindering our ability to invest and protect jobs in the Commonwealth. We urge the Patrick Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 so that the Department, Attorney General, regulated community and elected officials, can re-issue an entire set of rules by May 1, 2009, allowing for a two year period within which to implement the revised regulations.

We believe that successful implementation of regulations is necessary to protect personal information in the private and public sectors and to prevent further economic distress caused by the loss of personal data. However, these regulations place an unreasonable burden on already strained resources essential for success and growth of the Massachusetts economy.

As currently written, 201 CMR 17.00 goes beyond the legislature's intent through highly prescriptive mandates. For example, the legislature never intended to make encryption mandatory. In many instances the regulatory mandates are not technically or economically feasible. Further, the regulations do not envision the national and global business relationships that Massachusetts firms depend on.

The implications of 201 CMR 17.00 will have a negative impact on "all persons" and all firms that conduct business in Massachusetts. In sharp contrast, the state of New Jersey is currently in the process of implementing their data security laws, which includes a process of more than two years just to promulgate regulations not including actual implementation periods.

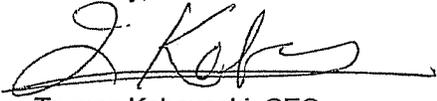
Regrettably, the Massachusetts regulations do not provide similar time, clarity, recognition of federal regulations nor do they recognize the significant technological, legal, operational challenges or the significant investments and human talent that many persons and small firms must now face.

The public sector must be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches.

Data security is not simple, no one person provide the expertise and no one technological solution will provide security. The Business Coalition, AIM and Energy Sciences, Inc., urge the Patrick Administration to provide an opportunity for greater stakeholder analysis with the business community, the Attorney General, regulated community and elected officials. We must get this right at the onset – cost effective data privacy rules that comply with the statute, set standards, recognize existing programs, and invite innovation

We respectfully urge the administration to allow for this process, to re-issue an entire set of rules with implementation of the rules over a two year period. Thank you for considering the long-term implications of these regulations for the protection of personal information of Massachusetts residents and the Massachusetts economy.

Sincerely,



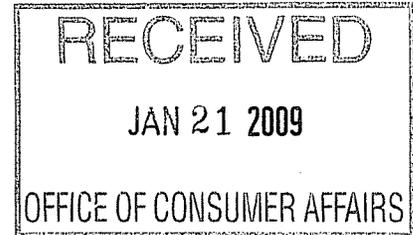
Tsuneo Kobayashi, CEO
Energy Sciences, Inc.



William Duserick
Chief Privacy Officer

January 21, 2009

Daniel Crane
Undersecretary
Office of Consumer Affairs and Business Regulation
Ten Park Plaza, Suite 5170
Boston, MA 02116



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

Dear Undersecretary Crane:

As a major employer in Massachusetts and one of the world's largest financial services companies, Fidelity Investments writes to express our serious concerns with *201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth*, promulgated by the Office of Consumer Affairs and Business Regulation ("OCABR") on November 14, 2008 (the "Regulations").

Fidelity takes the protection of the personal information it manages very seriously and supports the objective of the identity theft statute and the Regulations to improve the protection of the personal information of Massachusetts residents. We believe, however, that the Regulations impose costly new burdens on businesses and are inconsistent with existing national standards. The Regulations will result in a poorly timed imposition of unnecessary new business costs during a very challenging economic period and run counter to the Administration's initiative to improve the Massachusetts business climate through a streamlined regulatory scheme.

The business and operations of the financial services industry demand the extensive use of personal information. Such information is essential to completing financial transactions, and is required by myriad federal and state laws relating to taxes, health care, fraud prevention, homeland security, and securities. With more than 24 million customers who execute more than 90% of their transactions online, Fidelity has always considered the protection of sensitive information to be a foundation of customer trust and a sound business practice. We employ physical, electronic and procedural controls, and we regularly adapt and improve these controls to respond to changing requirements and advances in technology.

Not surprisingly, the breadth of new obligations imposed by the Regulations has given rise to a variety of different concerns for different organizations. Fidelity shares many of the concerns that a broad spectrum of companies and business organizations in Massachusetts and across the

country have raised about the substantive requirements of the Regulations and the challenging implementation timetable prescribed by OCABR.

In particular, we share the concern of many companies that the Regulations conflict with the underlying statute by imposing new obligations and restrictions that are inconsistent with existing federal laws. Pursuant to M.G.L. c. 93H (the "Statute"), OCABR is required to adopt implementing regulations that are designed to "insure the security and confidentiality of customer information in a manner fully consistent with industry standards." The Statute requires the OCABR's regulations to be "consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated." The Regulations clearly impose new obligations that are unique and specific to Massachusetts and create inconsistencies with both existing federal regulations and industry standards. These inconsistencies continue to raise concerns for Fidelity about the impacts on the multi-state operations of our business.

We would like to point out to you and your staff specific provisions of the Regulations where modifications or clarifying guidance from the OCABR would be helpful.

Service Provider Contract and Certification Requirements

The Regulations impose extensive requirements on entities that share the personal information of Massachusetts residents with third party service providers. Specifically, the Regulations require that prior to sharing personal information with any service provider, an entity must:

1. Verify that the service provider has the capacity to protect personal information;
2. Contractually require the service provider to maintain safeguards for personal information; and
3. Obtain from the service provider a separate written certification that the service provider is in compliance with the Regulations.

Separately, these contractual and certification requirements each can create significant obstacles and burdens for covered entities. Taken together, they represent a set of overlapping obligations that will require entities to engage in unnecessarily duplicative efforts and incur unwarranted costs while providing little or no added protection for Massachusetts residents.

Given its size and the complexity and scope of its business, Fidelity has hundreds of service providers entrusted with personal information. These service providers serve necessary and important functions, such as statement printing and mailing, customer check writing and bill paying services, data processing, professional services, and meeting various regulatory obligations, as well as providing workplace benefits, background checks and other services with respect to Fidelity's employees. Like many companies, it is critical that Fidelity is able to engage and interact with service providers in ways that are efficient and appropriately regulated in light of the national marketplace in which we operate. Single-state requirements like those in the Regulations ignore these necessities.

Service Provider Certifications

Section 17.03(f) requires every entity that shares personal information with service providers to obtain from each service provider a written certification that the provider is in compliance with

the Regulations. This obligation is unique and unprecedented, and it is inconsistent with industry standards and existing federal regulations under which Fidelity operates.

While a number of federal regulators have required entities to contractually obligate their service providers to protect customers' personal information, we are aware of no other regulator that has required a separate written certification as required by the Regulations. We appreciate OCABR's decision to delay the implementation date of this provision of the Regulations to January 1, 2010. But despite the delay, the imposition of this Massachusetts-specific certification requirement will continue to create a costly regulatory obligation which is inconsistent with national industry practice and standards, particularly for companies that operate in interstate commerce. Soliciting and obtaining certifications from all of its impacted service providers will be an immensely costly and burdensome exercise for Fidelity and other companies. We believe that the service provider selection standards required by the Regulations, coupled with an effective and flexible approach with regard to requiring certain contract language to be included in contracts with service providers, are more than sufficient to effectively ensure the safety of personal information shared with service providers. To also require a separate certification would be unwarranted and unnecessarily duplicative.

Additionally, the service provider certification requirement can cause circular compliance (or non-compliance) issues for companies that both retain and provide vendor services. Fidelity, in its role as a service provider, will not be able to certify to its clients that it is compliant with the new state law and the Regulations until it receives certifications from all of its service providers with whom it shares personal information. This type of circularity can be avoided by utilizing contractual provisions to impose safeguarding requirements on service providers.

We strongly urge the OCABR to amend the Regulations to remove the vendor certification requirement and require instead a contractual language requirement on a prospective basis. This is a more flexible approach that reflects the realities of the multi-state and multi-national markets in which many companies operate. If OCABR maintains the vendor certification requirement in the Regulations, we request that it remove the duplicative contractual safeguard requirements in Section 17.03(f). Alternatively, a separate vendor certification could serve as a substitute that entities may choose to utilize if they do not or cannot satisfy the contractual language requirement.

Contractual Safeguard Requirement

Section 17.03(f) requires entities that share personal information with service providers to contractually require the service provider to maintain safeguards for personal information. We believe that many existing service provider contracts include language that appropriately and effectively obligate vendors to safeguard personal information through "compliance with law" provisions and with specific provisions that are compliant with the requirements of the SEC's Regulation S-P.

The type of service provider contract requirement that is imposed by Section 17.03 is not unprecedented. As previously mentioned, several federal regulators, including the Securities and Exchange Commission (SEC) and the U.S. Department of Health and Human Services (HHS), have imposed similar requirements. OCABR's application of the requirements in Section 17.03 could, however, result in unprecedented impacts to companies like Fidelity, particularly if OCABR insists on imposing obligations of single-jurisdiction specificity. We believe it is critical that OCABR allow general contract language that is not specific to Massachusetts or any

other state to satisfy this contractual safeguard requirement. To do otherwise will create a landscape where each successive change to the statute or regulation in any state could require subject entities to amend vast numbers of contracts.

Like many commercial contracts, our contracts typically contain language that requires service providers to comply with any and all applicable state laws. These types of overarching, “compliance with law” provisions reflect the commercial realities of the ever-changing regulatory landscape businesses operate under and are designed to avoid the very type of never-ending amendment cycle that Section 17.03 would create.

Many of our existing service provider contracts also specifically require our service providers to treat customer information confidentially. Under the Gramm-Leach-Bliley Act, the SEC has promulgated Regulation S-P, which requires Fidelity and other regulated entities to enter into contractual agreements prohibiting third party service providers from disclosing or using nonpublic personal information other than to carry out the purposes for which the information has been provided. We believe that contract provisions that comply with the requirements of the Gramm-Leach-Bliley Act do and should fulfill the Regulation’s contractual safeguard requirement. We request that OCABR modify the Regulations or issue guidance to confirm and clarify this interpretation.

If OCABR insists on imposing additional Massachusetts-specific contract requirements, then it should apply any such requirements only on a prospective basis. In this way, companies can avoid the extensive costs associated with negotiating amendments to a large number of existing service provider contracts. Requiring entities to amend scores of existing vendor contracts is extremely burdensome and wasteful, particularly if existing contracts already include language that protects customers and complies with existing federal standards. Requiring such contract amendments would be even more wasteful if OCABR continues to require that these same vendors will be obligated to provide certifications just a few months later.

We understand and appreciate OCABR’s interest in protecting the Commonwealth’s residents by ensuring that entities that maintain Massachusetts resident information do not carelessly share that information with third party service providers. But we believe that the Regulations could continue to serve this underlying purpose by allowing companies to satisfy either a contractual requirement or a certification requirement and permitting companies to satisfy the contractual safeguards requirements with certain existing and widely-used contract provisions.

Portable Device Definition

Section 17.04(5) of the Regulations requires the encryption of all personal information stored on laptops or other “portable devices.” This remains an unclear mandate – one that has not been imposed by any other state law or regulation. We believe that the term “portable devices” refers only to actual devices, such as Blackberries and Personal Digital Assistants, rather than to other storage media, such as discs or tapes. A broader interpretation of this term would require a costly and burdensome encryption process that would offer little additional protection to the consumer. We respectfully request that OCABR provide interpretive guidance to clarify that the term “portable device” refers only to an actual device that by itself allows a user of the device to access information stored on the device.

Conclusion

In conclusion, we believe that both economic realities and the Statute require that OCABR promulgate regulations that recognize and are consistent with the many federal regulatory layers already imposed on the companies that do business in Massachusetts. The legislature recognized the crucial need to avoid Regulations that might unnecessarily impede businesses, particularly Massachusetts businesses, from operating and competing in a global marketplace. It is critical that the implementing regulations do not create conflicting standards and obligations that would cause competitive disadvantages to impacted companies.

We appreciate the opportunity to share these concerns with you and to continue to discuss workable solutions that will protect the personal information of the residents of the Commonwealth without imposing any unnecessarily burdensome requirements on Massachusetts businesses and employers.

Sincerely,



William Duserick
Chief Privacy Officer
Fidelity Investments

Cc: Daniel O'Connell, Secretary of Housing and Economic Development

January 21, 2009

Governor Deval Patrick
Massachusetts State House
Office of the Governor
Room 360
Boston, MA 02133
Phone: 617.725.4005
Fax: 617.727.9725

Secretary Daniel O'Connell
Daniel Crane, Undersecretary
David Murray, General Counsel
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116
p. 617-973-8700
f. 617-973-8799
Email: David.Murray@state.ma.us

CC: Senator Jennifer Flanagan, Representative Dennis Rosa, North Central
Massachusetts Chamber of Commerce

Top Priority: Protect Personal Information through Stakeholder Analysis

Dear Governor Patrick, Secretary O'Connell and Undersecretary Crane:

As an employer with approximately 140 employees, I am very concerned, about the mandates in 201 CMR 17.00. These regulations set a perilous course for my business, the state and our shared goals to invest and protect jobs in the Commonwealth. I urge the Patrick Administration to engage in a rigorous stakeholder analysis and transparent comment process focused on the entire set of regulations within 201 CMR 17.00 with the Department, Attorney General, regulated community, and elected officials with a goal issue an entirely new set of rules by May 1, 2009 with implementation over a two year period.

The protection of personal information for residents of the Commonwealth is a top priority for everyone. The delay in the effective date is helpful, as a practical matter, but it is unreasonable to believe that my firm or others have a fair opportunity to reach full compliance. As currently written, 201 CMR 17.00 goes beyond the legislature's intent and mandates specific technologies, creates redundant and confusing rules and does not hold public agencies to the same standards of the private sector. In many instances the regulatory mandates are not technically or economically feasible for public or private agencies regardless of size or available resources. Further, the regulations do not envision the national and global business relationships that the Massachusetts economy depends on.

The current rules will have a negative impact on “all persons” and all firms that conduct business in Massachusetts. The promulgation and implementation history of these specific regulations are in sharp contrast with other states and even other Massachusetts state agencies that routinely engage in extensive and vibrant collaborative discussions with the regulated communities. The state of New Jersey recognized the need for a vigorous stakeholder analysis. Currently, the State of New Jersey is engaged in a two-year process just to promulgate a “pre-proposal” for data privacy regulations and that does not include the phase in time for actual compliance. Regrettably, the Massachusetts process for our privacy regulations did not provide similar time, clarity, education, and recognition of federal regulations, nor do the rules recognize the significant technological, legal, operational challenges, or the significant investments and human talent that many persons and small firms must now face.

The following is a partial list of the issues and solutions that the business community has identified:

Time: Time is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules to achieve the ultimate goal of compliance. The resulting regulations should be implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community.

Consistency: Consistency with existing and soon to be promulgated federal law and the laws of other states is essential, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict other federal and state laws and provide little or no additional substantive protection for Massachusetts consumers, employees and other residents.

Contract provisions and written certifications: The third party contractual obligations and separate certification are duplicative, confusing, and unnecessary. Contractual language requiring third parties holding personal data to protect such information should be used, not certification. Otherwise the contract obligations and written certification requirements becomes a never ending, complex, costly, and essentially circular mandate virtually without end.

Mandatory encryption: Encryption of data is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard the Legislature put in the law. A standard for the outcome protecting personal data should be used allowing the regulated community to develop a range of measures for protection, rather than complying with a single command and control technology requirement.

Inventory: The inventory requirement to find every piece of personal data is a complex, costly and counterproductive effort, drawing resources away from more important

privacy objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated. A better, more meaningful approach is to undertake a risk analysis of systems identifying the potential for the loss of such data. The risk assessment approach would be similar to what is required in other federal and state contexts.

Information collected and time held: Data collecting and holding requirements are problematic and the regulatory structure does not require such rules. Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy.

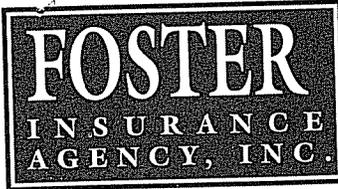
Public sector: Massachusetts agencies need to be held to exactly the same standards as the private sector for data privacy. Personal data is regularly shared with public entities and has the potential to be a source of significant data breaches. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose.

In the final analysis, under the existing rules "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 to "all persons" or firms, regardless of available resources.

Data security is not simple, no one person in a firm can provide the expertise, and no single technological solution will work in all situations. We must get this right – cost effective data privacy rules that comply with the statute, set standards, recognize existing programs, and invite innovation. Thank you for considering the long-term implications of these regulations and their direct impact on my business and the Massachusetts economy.

Sincerely,

Michael A. Quirk
Human Resources Manager
Fosta-Tek Optics, Inc.
Leominster, MA

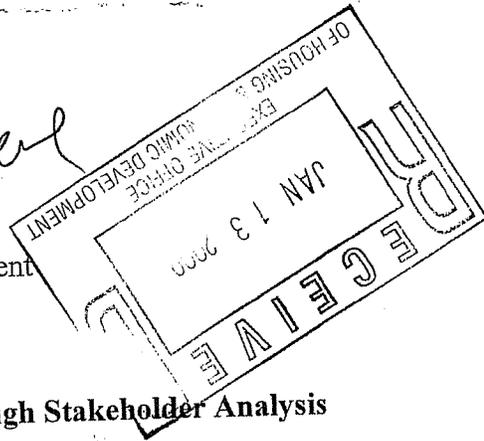


AGENTS
BROKERS
RISK MANAGEMENT
CONSULTANTS

January 9, 2009

To: Dan O'Connell

Secretary Daniel O'Connell
Executive Office of Housing & Economic Development
One Ashburton Place, Room 2101
Boston, MA 02108



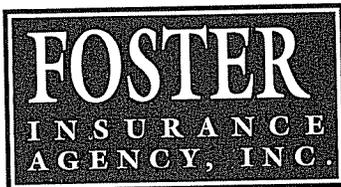
Top Priority: Protect Personal Information through Stakeholder Analysis

Dear Secretary O'Connell,

As an employer with 14 employees, I am very concerned, about the mandates currently included in 201 CMR 17.00. As written, these regulations set a perilous course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth. I urge the Patrick Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 with the Department, Attorney General, regulated community and elected officials, to re-issue an entire set of rules by May 1, 2009 with implementation of the rules over a two year period.

As a business owner or employee the protection of personal information for residents of the Commonwealth is a top priority. The delay in the effective date is helpful, as a practical matter, it is unreasonable to believe that my firm has a fair opportunity to reach full compliance. As currently written, 201 CMR 17.00 goes beyond the legislature's intent and mandates specific technologies, creates redundant and confusing rules and does not hold public agencies to the same standards of the private sector. In many instances the regulatory mandates are not technically or economically feasible for public or private agencies regardless of size or available resources. Further, the regulations do not envision the national and global business relationships that the Massachusetts economy depends on.

The implications of 201 CMR 17.00 will have a negative impact on "all persons" and all firms that conduct business in Massachusetts. The promulgation and implementation of these specific regulations are in sharp contrast with other states and especially other Massachusetts state agencies that routinely engage in collaborative discussions with the regulated communities. The state of New Jersey recognized the need for a vigorous stakeholder analysis.



AGENTS
BROKERS
RISK MANAGEMENT
CONSULTANTS

Currently, the State of New Jersey is currently in a two year process just to promulgate a "pre-proposal" of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey's new pre-proposal provides for a comment period until February 13, 2009. Regrettably, the Massachusetts regulations do not provide similar time, clarity, recognition of federal regulations nor do they recognize the significant technological, legal, operational challenges or the significant investments and human talent that many persons and small firms must now face.

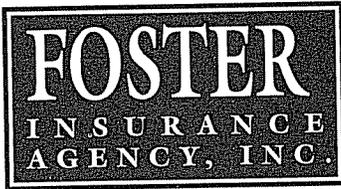
The following is a partial list of the issues and solutions that the business community has identified:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules to achieve the ultimate goal of compliance. The regulations should be implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Otherwise the contract and written certification requirement becomes a never ending, complex, costly, and circular mandate virtually without end.

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute. A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology.



AGENTS
BROKERS
RISK MANAGEMENT
CONSULTANTS

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated. A better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. The risk assessment approach would be similar to what is required in other federal and state contexts.

Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations. Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy

Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose

Under these rules "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 to "all persons" or firms, regardless of readily available resources.

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. Thank you for considering the long-term implications of these regulations and their direct impact on my business and the Massachusetts economy.

Sincerely,



Scott W. Foster, President CPCU
Foster Insurance Agency, Inc.
321 Lunenburg Street
Fitchburg, MA 01420

Governor Deval Patrick
Massachusetts State House
Office of the Governor
Room 360
Boston, MA 02133

Big Problems with New Regulations to Protect Personal Information

Dear Governor Patrick:

As an employer with 30 employees, I am very concerned about the mandates currently included in 201 CMR 17.00. As written, these regulations set a perilous course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth. I urge the Patrick Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 with the Department, Attorney General, regulated community and elected officials, to re-issue an entire set of rules by May 1, 2009 with implementation of the rules over a two year period.

As a business owner or employee the protection of personal information for residents of the Commonwealth is a top priority. The delay in the effective date is helpful, as a practical matter, it is unreasonable to believe that my firm has a fair opportunity to reach full compliance. As currently written, 201 CMR 17.00 goes beyond the legislature's intent and mandates specific technologies, creates redundant and confusing rules and does not hold public agencies to the same standards of the private sector. In many instances the regulatory mandates are not technically or economically feasible for public or private agencies regardless of size or available resources. Further, the regulations do not envision the national and global business relationships that the Massachusetts economy depends on.

The implications of 201 CMR 17.00 will have a negative impact on "all persons" and all firms that conduct business in Massachusetts. The promulgation and implementation of these specific regulations are in sharp contrast with other states and especially other Massachusetts state agencies that routinely engage in collaborative discussions with the regulated communities. The state of New Jersey recognized the need for a vigorous stakeholder analysis. Currently, the State of New Jersey is currently in a two year process just to promulgate a "pre-proposal" of regulations that do not yet specify actual implementation deadlines. In fact, on December 15,

2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey's new pre-proposal provides for a comment period until February 13, 2009. Regrettably, the Massachusetts regulations do not provide similar time, clarity, recognition of federal regulations nor do they recognize the significant technological, legal, operational challenges or the significant investments and human talent that many persons and small firms must now face.

The following is a partial list of the issues and solutions that the business community has identified:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules to achieve the ultimate goal of compliance. The regulations should be implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Otherwise the contract and written certification requirement becomes a never ending, complex, costly, and circular mandate virtually without end.

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute. A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology.

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated. A better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. The risk assessment approach would be similar to what is required

in other federal and state contexts.

Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations. Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy

Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose

Under these rules "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 to "all persons" or firms, regardless of readily available resources.

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. Thank you for considering the long-term implications of these regulations and their direct impact on my business and the Massachusetts economy.

Sincerely,

G. L. (Lee) Gaudette, III, CPCU
President

cc: Daniel.OConnell@state.ma.us; dan.crane@state.ma.us; David.Murray@state.ma.us; Michael.W.Morrissey@state.ma.us; Richard.Moore@state.ma.us; Rep.MichaelRodrigues@hou.state.ma.us; Rep.GeorgePeterson@Hou.State.MA.US; Rep.JenniferCallahan@hou.state.ma.us

**Testimony of the Greater Boston Chamber of Commerce
Before the Office of Consumer Affairs and Business Regulation
January 16, 2009**

The Chamber would like to submit testimony on behalf of its 1,700 members, all of which will be impacted by the proposed data privacy regulation, *Standards for the Protection of Personal Information of Residents of the Commonwealth* [210 CMR 17.00].

First, the Chamber would like to thank the Administration, the Attorney General's office, and the legislature for their ongoing efforts on this important matter. We would also like to acknowledge and applaud the decision last fall by the Office of Consumer Affairs & Business Regulation to delay effective dates for this regulation. Such delays were absolutely essential for companies seeking to become compliant with this unprecedented set of new data privacy requirements.

Ensuring data privacy is a goal we all share, and we believe this issue can be addressed in regulation without significantly impacting jobs, investment, or the overall economic competitiveness of the state. Implementation delays are a very positive step in that direction – however, there are requirements within the regulation that we believe merit further discussion and consideration prior to their effective dates:

DEFINITIONS

Personal information: While the definition in the regulation appears straight-forward, there remains uncertainty among several industries as to whether other customer data would be included in this definition, either through interpretation or enforcement. A commonly-used example is that of “customer account numbers” such as are used by utilities. While not explicitly cited in the regulation, companies are concerned that such account numbers would be treated in the same way as social security or financial account numbers. Unlike those numbers, customer account numbers cannot be used to withdraw funds or establish someone else's identity. Excluding “customer account numbers” from the definition of “personal information” would remove this uncertainty and ensure that such account numbers are not subject to the statute and the regulations.

- **Recommendation:** At the end of the last sentence of section 17.02, subsection (c) in the definition of *Personal Information*, insert “, nor shall it include non-financial customer accounts numbers.”

ENCRYPTION

Going-forward basis: We believe encryption should be required only on a going forward basis for any new investment, upgrade or equipment purchase. New systems could be encrypted in many situations at additional cost, but adding encryption capabilities retroactively to systems and devices purchased even just a few years ago could be very difficult and costly. We recommend inserting language that requires encryption on systems and devices acquired or implemented after the effective date of the regulation.

- **Recommendation** – Revise subsection (3) of section 17.04 by inserting the following sentence thereafter: “Encryption requirements in this regulation are applicable to devices, networks, and systems acquired or implemented after the effective date of this regulation.”

Flexibility in technology: In addition, prescribing specific encryption technologies would prevent companies from employing cutting-edge solutions in this rapidly evolving field. Our understanding is that the regulation was not intended to be overly prescriptive in terms of which technologies are used, as long as the result is the encryption of personal information. Such latitude would enable network-based content blocking, portable device-disabling “kill pills”, and other next-generation technologies to be used to meet the requirement. We agree with this thoughtful approach and urge its codification in the regulation.

- **Recommendation:** Insert language allowing technological flexibility in meeting encryption requirements of this regulation.

Clarifying requirements for wireless systems: We urge a revision ensuring that encryption requirements for wireless systems and devices do not exceed the intended scope of the regulation. Such a revision would preserve encryption requirements for “transmitted records and files containing *personal information* that will travel across public networks,” but would protect against an interpretation in which the regulation is deemed applicable to other wirelessly transmitted data such as internet packets or emails (that contain no personal information).

- **Recommendation:** Strike the last clause in subsection (3) of section 17.04.

INVENTORY

For most companies, the compliance process could take months and even years to complete and will involve substantial new up-front costs. Also, due to the evolving nature of data stores and systems, an inventory of the location of every personal data point for Massachusetts residents would have to be continuously updated, thereby imposing significant ongoing costs and drawing critical resources away from more important privacy objectives. We recommend an approach that reflects these realities:

- **Recommendation:** Inserting at the beginning of subsection (h) of section 17.03 the following: “Companies are permitted to conduct an assessment of the data they retain and the potential loss of such data. Determinations of compliance with this provision will be based on inserting language that allows companies to adopt a more risk-based approach grounded in the data they keep and the potential for the loss of such data.”

THIRD-PARTY VENDOR CERTIFICATION

When dealing with third-party vendors, companies typically insist on and negotiate contractual language guaranteeing the safety and security of their customers’ personal information. Best practices such as this are essential to securing a company’s reputation, long-term viability, and commitment to its customers. Many of our larger companies have hundreds upon hundreds of vendor contracts currently in place – the prospect of having to reopen or renegotiate existing contracts in order to satisfy the vendor certification process in this regulation would prove immensely costly, time-consuming and, in many cases, unworkable – especially if vendors are located outside of Massachusetts, are the only vendor offering a certain product or service in this market, or are simply unwilling to certify compliance to a new code while under an existing contract.

- As such, we recommend removing third-party vendor certification requirements – **striking the last sentence of subsection (f) in section 17.03** – in favor of a process in which companies are required to only certify their own compliance.

If the removal of third-party certification cannot be accommodated in the regulation, we strongly urge the following revisions to at least ensure that such a process is workable:

Eliminate retroactivity of vendor certification, requiring such certifications only as part of new contract agreements inked after the regulation becomes effective. Requiring certification on a “going-forward” basis is consistent with the allowances made for public agencies in Executive Order 504, *Order Regarding the Security and Confidentiality of Personal Information*. If public agencies are allowed to certify vendors only on a going-forward basis, companies should be governed by the same principle.

- **Recommendation** – Strike “After January 1, 2010” in subsection (f) in section 17.03 and insert the following at the end of this revised last sentence in subsection (f): “The requirements of this provision are applicable to agreements finalized after the effective date of this regulation.”

Insert language to only require a company to obtain compliance certification from the vendors they directly contract with. It is our understanding that limiting such a requirement to just the company and their direct vendor was intended by OCABR in its drafting of the regulation, however codifying language in the regulation would provide certainty to companies engaging in multi-party transactions – such as routinely occurs in financial services – that they need not certify each vendor that their primary vendor utilizes in order to execute a transaction.

- **Recommendation** – Insert the word “direct” before the term “third-party service providers” anywhere it appears in subsection (f) in section 17.03.

PERSONAL INFORMATION COLLECTION

The collection and retention of personal customer information has long been a standard and essential business practice of companies of all size and industry. Overly restrictive limits on both the amount of information that can be collected and the time that such information can be retained could disrupt long-standing operational processes at companies, while limiting marketing, advertising and customer service options and placing Massachusetts companies at a distinct competitive disadvantage. Furthermore, if companies are compliant with a first-in-the-nation regulation securing and protecting all sensitive or material personal information, limits on the amount of information collected and the time it can be retained would be unnecessary.

- **Recommendation** – Strike subsection (g) of section 17.03 within the regulation.

SMALL BUSINESS COMPLIANCE CHECKLIST

While we greatly appreciate the responsiveness of OCABR to address the substantial compliance concerns that persist in the small business community, we believe that implementing a great many of the items on this checklist would prove unworkable or cost-and-resource prohibitive for small businesses. Recognizing the already substantial hurdles most small businesses must overcome simply to remain in business these days, the Chamber believes the checklist should be presented as a “set of possible options” for small businesses or individuals to consider, rather than a prescriptive set of items that not only exceed the scope of the regulation, but “require attention in order for a plan to be compliant.” Such a revision would reflect the intent of the regulation and its allowances for compliance scalability based on size, scope, type of business, available resources, and need for data security and confidentiality.

- **Recommendation** – Strike the last sentence in the first paragraph of *201 CMR 17.00 Compliance Checklist* and replace with: “The following items, in question and answer, may be considered as options by small businesses or individuals in evaluating their plan for compliance.”

In closing, this regulation will impact companies of all sizes and industries at a time of widespread budgetary constraints and accelerating revenue and job loss. The cost and operational burden of any new business regulation must be viewed, in part, through this lens. In addition, lack of awareness persists among many employers, and uncertainties about compliance and impacts remain among those employers who are aware of these new requirements. As such, the Chamber looks forward to continuing this discussion in the weeks ahead and working toward implementing a data privacy regulation that furthers our commonly shared goals of protecting personal information and growing the economy.

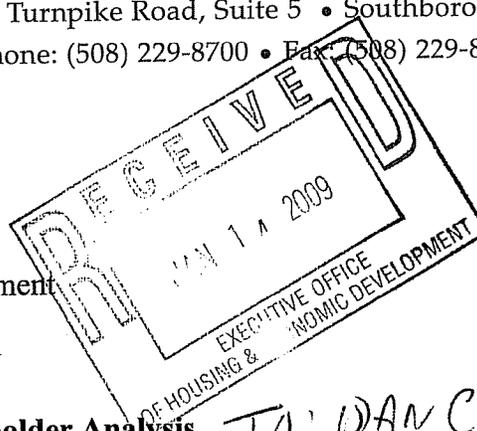


Hayden Wood
Insurance Agency, Inc.

30 Turnpike Road, Suite 5 • Southborough, MA 01772
Phone: (508) 229-8700 • Fax: (508) 229-8702

January 12, 2009

Secretary Daniel O'Connell
Executive Office of Housing & Economic Development
One Ashbuton Place, Room 2102
Boston, MA 02108



Re: Protect Personal Information through Stakeholder Analysis

TO: DAN CRANE

Dear Secretary O'Connell,

I am writing to you today as a local small business owner who currently employs 5 full time and 2 part time employees, has been conducting business here in Massachusetts since 1946 and am very concerned about the mandates currently included in 201 CMR 17.00. As written, these regulations set a perilous course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth. I urge the Patrick Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 with the Department, Attorney General, regulated community and elected officials, to re-issue an entire set of rules by May 1, 2009 with implementation of the rules over a two year period.

In today's society the access to personal information and the misuse of such is at the forefront of day to day operations in any small business. As the owner of a small business the protection of my client's personal information is a top priority. The delay in the effective date is helpful, as a practical matter, it is unreasonable to believe that my company has a fair opportunity to reach full compliance. As currently written, 201 CMR 17.00 goes beyond the legislature's intent and mandates specific technologies, creates redundant and confusing rules and does not hold public agencies to the same standards of the private sector. In many instances the regulatory mandates are not technically or economically feasible for public or private agencies regardless of size or available resources, especially in these troubling financial times. Further, the regulations do not envision the national and global business relationships that the Massachusetts economy depends on.

The implications of 201 CMR 17.00 will have a negative impact on "all persons" and all firms that conduct business in Massachusetts. The promulgation and implementation of these specific regulations are in sharp contrast with other states and especially other Massachusetts state agencies that routinely engage in collaborative discussions with the regulated communities. The state of New Jersey recognized the need for a vigorous stakeholder analysis. Currently, the State of New Jersey is currently in a two year process just to promulgate a "pre-proposal" of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and



GENERAL INSURANCE • HOMEOWNERS, AUTO, BUSINESS & BONDS
www.haydenwood.com



withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey's new pre-proposal provides for a comment period until February 13, 2009. Regrettably, the Massachusetts regulations do not provide similar time, clarity, recognition of federal regulations nor do they recognize the significant technological, legal, operational challenges or the significant investments and human talent that many persons and small firms must now face.

The following is a partial list of the issues and solutions that the business community has identified:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules to achieve the ultimate goal of compliance. The regulations should be implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Otherwise the contract and written certification requirement becomes a never ending, complex, costly, and circular mandate virtually without end.

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute. A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology.

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated. A better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. The risk assessment approach would be similar to what is required

in other federal and state contexts.

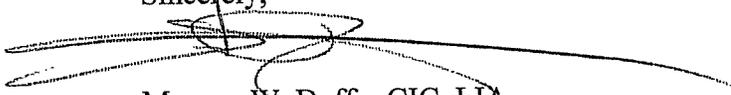
Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations. Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy

Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose

Under these rules "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 to "all persons" or firms, regardless of readily available resources.

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. Thank you for considering the long-term implications of these regulations and their direct impact on my business and the Massachusetts economy.

Sincerely,



Morgan W. Duffy, CIC, LIA
President – Hayden Wood Insurance Agency, Inc.

CC: Local Legislators, (Karyn Polito, Michael W. Morrissey & Michael J. Rodrigues)

Joint Committee on Consumer Protection and Professional Licensure

201 CMR 17.00

Testimony of Joe Moore, Executive Director International Health, Racquet & Sportsclub Association (IHRSA)

January 16, 2009

Members of the Committee, thank you for the opportunity to submit testimony on the amendments to 201 CMR 17.00, *Standards for the Protection of Personal Information of Residents of the Commonwealth*, which would extend the compliance date for obtaining certification from third party service providers to January 1, 2010, and for encrypting portable devices other than laptops to May 1, 2009.

My name is Joe Moore, and I am the Executive Director for the International Health, Racquet & Sportsclub Association (IHRSA), the leader in education, research and advocacy for the health and fitness industry. IHRSA represents 187 health clubs throughout Massachusetts, 7,000 worldwide, and we are opposed to these amendments as currently written.

First of all, I would like to thank you for taking the time to address an issue that is critical to the business community: the ever-growing need for greater protection and security of personal information. As technology becomes more advanced and information is shared at a faster and more frequent pace, businesses must go to greater lengths to ensure that the confidentiality of such information is not jeopardized. We recognize the good intentions of the sponsors of these amendments, and the members of this Committee, who clearly have the safety of all Massachusetts residents in mind.

However, I am concerned that the amendments, as currently written, are not technically or economically feasible in the time that is allotted for compliance. Compliance with these regulations will require a significant amount of financial resources, time and personnel, on behalf of all health clubs. Although the delay in the effective date is helpful, roughly five months to execute all necessary steps and acquire the necessary resources (financial and otherwise) does not give clubs a fair opportunity to reach compliance.

The immediacy of the financial investment that would be required to reach compliance would place an enormous strain on health clubs, many of who are already struggling during this difficult economic period. While these regulations are well intentioned, they could exacerbate the fiscal strain that is currently on our economy. Also, business size is not indicative of operational costs. Many smaller health clubs do not have the financial resources to invest in costly encryption hardware and software.

Further extending the compliance date will allow time to ensure that all health clubs are aware of and understand the regulations. We support the idea that health clubs would benefit from greater clarity regarding compliance according to company size and available resources. This will decrease the risk of clubs being out of compliance and having to face penalties.

I thank the Committee for your time and I would be happy to answer any questions that you may have.

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 Association¹ 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,

A handwritten signature in black ink that reads "Paul D. Glenn". The signature is written in a cursive, flowing style.

Paul D. Glenn
Counsel

**TESTIMONY OF THE INVESTMENT COMPANY INSTITUTE
BEFORE THE OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION**

My name is Tami Salmon and I am here today representing the mutual fund members of the Investment Company Institute. The Institute is the national association of the U.S. mutual fund industry. Members of the Institute operate in all 50 states, as well as internationally; they manage total assets of almost \$10 trillion; and they serve over almost 93 million shareholders. As regards the Commonwealth, approximately half of the households here own at least one mutual fund and these shareholders account for approximately \$290 billion in mutual fund assets.

Massachusetts remains the epicenter of the mutual fund industry with Massachusetts investment companies managing \$2.4 trillion in assets, or 21% of the total industry assets. Importantly, these companies are also large employers in the Commonwealth, employing over 33,000 persons, or approximately 20% of the total employees in the industry. Many of the Institute's members have joined me here today. It is because of the importance of the Commonwealth to the mutual fund industry, and the industry's concerns with the new data security standards that I am here today to discuss the recent extension of the compliant date attached to the Standards.

As a preliminary matter, I want to stress that mutual funds have long taken seriously their obligation to protect the confidentiality and integrity of non-public consumer information. This obligation derives not only from requirements imposed on us under Federal law, but on each fund's interest in protecting its brand image. Our industry depends on investors' trust to survive and an important component of that trust is protecting the confidentiality, security, and integrity of shareholders' information, regardless of where that shareholder may reside. It is for this reason that our members have spent tens of millions of dollars on their information security systems and why they continue to revise them as necessary to ensure they address new and emerging vulnerabilities and threats, and adopt security new technologies as appropriate.

Notwithstanding that commitment to data privacy, I am here today both to express the very serious concerns our members have with the manner and substance with which the Department of Consumer Affairs and Business Regulation undertook rulemaking under Chapter 93H and to comment on the emergency rules issued in December. As you know, my appearance today is not the first time the Institute has expressed these concerns.

To recap briefly, we first expressed concerns with the proposed rules on January 10, 2008. Shortly after their adoption, by letter dated October 8, 2008, we expressed our concerns with their extra-territorial impact and their aggressive compliance date. On November 17th, I met with representatives of the Department along with 17 mutual fund companies to again express our serious concerns with the overly prescriptive requirements of the rules and the aggressive compliance date. On November 19th, I testified before the Legislature's Joint Committee on Consumer Protection and Professional Licensure regarding our concerns with the rules. On November 26th, at the request of the Department as a follow-up to our November 17th meeting, I filed a lengthy letter with the Department on behalf of mutual funds identifying very specific issues of concern, including the compliance date, and seeking clarification of various requirements. On December 12th, after attending the conference of the National Association of State Treasurers, where the Standards were discussed in detail and state officials expressed serious concerns with their potential application to such states' activities, I again wrote to the Department. My last letter to the Department, which was sent on December 24th identified each of the issues from our November 26th letter that the Department either failed to address or did not address in a meaningful way.

I provide this history by way of background regarding our efforts to clearly present to the Department the serious concerns mutual funds have with the prescriptive, vague, and impractical provisions comprising the Standards. Because these efforts, to date, have been largely unsuccessful in opening a fruitful dialogue with the Department, I am here again today, to reiterate these concerns in the context of the emergency rules.

Since today's hearing is ostensibly focused on the Department's recent extension of the compliance dates attached to the Standards, I want to first address this issue. When we met with you on November 17th, we expressly asked you how the Department determined the new compliance date and who the Department has consulted to determine their appropriateness. From the response we received, it appears that the Department did not consult anyone from the private sector but determined the new dates were reasonable. We respectfully disagree with your determination. As presented in our previous correspondence, we know from our direct experience implementing Federal rules that, to the extent they can be implemented, **it will take mutual funds a minimum of two years to implement fully the Standards' requirements.**

Notwithstanding the absence of its own empirical evidence, the Department “believes,” that we can accomplish compliance by May 1st for all provisions in the Standards except encryption of portable devices and receipt of certifications, which it believes we can comply with by January 1, 2010. The Department has also indicated that the May 1st compliance rule is intended to enable persons to implement the rules at the same time they implement the Federal Trade Commission’s new “Red Flag Guidelines,” which also have a compliance date of May 1st. This presumably reflects the idea that the two regulatory systems are somehow linked and some efficiency flows from the choice of a joint compliance deadline. We find aligning these two compliance dates to be most peculiar in light of the fact that there are no regulatory similarities between the Massachusetts rules and the FTC’s rules. Moreover, many persons subject to Massachusetts’ rules – including many mutual fund companies – are not subject to the FTC’s rules because they do not permit third-party payment from their shareholders’ accounts. Accordingly, we are at a loss to understand why, in the Department’s view, it is appropriate to link any compliance date for its rules to the FTC’s compliance date. We would add, however, that for those companies that are subject to the FTC’s rule, the FTC has provided a compliance period of 18 months - which is far more time than the

Department is providing persons to comply with its rules, even though the FTC's rules are far less complex than the Department's rules.

While I know, based upon a Department letter to me, that the Department believes our members should have begun implementing the rules as soon as they were proposed for comment a year ago, such a response undermines the public comment process. I am not aware of any business that would expend considerable time, energy, and resources on rule requirements that may or may not be adopted some day.

Because mutual funds' concerns are well documented through our previous correspondence, meetings, and testimony, I will not waste your time today by dwelling on them in any great detail. I will, however, provide them in hard copy this afternoon so that they become part of the administrative record of this rule making. Given the nature of this hearing, which is the question on an appropriate time frame for these regulations, I believe it appropriate to outline for the record the nature of these concerns and suggest to you that compliance dates of May 1st and January 1st, 2010 are not appropriate because of the complexity of these issues:

- **First**, the rules appear to exceed the Department's statutory authority because they are not "consistent with" federal law as required by Chapter 93H. Nor do the rules provide sufficient flexibility based on a person's size, scope, type of business, amount of resources, amount of stored data, and need for the security and confidentiality of information as also required by Chapter 93H;
- **Second**, the rules will impede interstate commerce because they will preclude the free movement of information until persons wholly outside the Commonwealth are willing to subject themselves to the Commonwealth's requirements and affirm so in writing;
- **Third**, contrary to the Commerce Clause of the U.S. Constitution, the rules appear to impermissibly subject other states to the Commonwealth's regulatory requirements and enforcement authority and, as I have already personally heard, your sister states are not willing to submit to your authority and have no intention of receiving only encrypted information, modifying their contracts with our members or others to affirm their compliance with Massachusetts law, or providing certifications regarding their compliance as the Standards require them to do; and

- **Fourth, the rules** are overly prescriptive and take a one-size-fits-all approach to data security, which makes them difficult to implement and, ironically, less effective. The difficulty mutual funds, among others have in implementing the rules is exacerbated by the Department's unwillingness or inability to address very specific issues raised by the rules – for example, who is a third-party vendor?

Without knowing *with precision the answer* to this question, persons subject to the rules cannot implement them with any degree of compliance certainty.

These comments highlight but a few of our concerns with the rules and the deficiencies in the emergency amendment to them issued last December. Other concerns we have raised with the Department that remain unresolved include provisions in the rule relating to encryption, the definition of key undefined terms, and the meaning of ambiguous provisions. Each of these have been amply documented in our correspondence to the Department.

In closing, I want to briefly raise two additional issues, one of which I understand was raised by Senator Morrissey in a recent letter to Secretary O'Connell and relates to the economic impact of implementing the Standards. I continue to see quotes in the press from Department regarding the *de minimis* fiscal impact of the Standards and I

believe that, if the Department believes its own quotes, it needs to undertake a far more rigorous analysis of the fiscal impact of the Standards than it has done to date. Our members expect to spent millions of dollars implementing the rules. Indeed, the testimony presented at the December legislative hearing indicated the serious concerns businesses – from the smallest companies to the largest – have with the costs they will incur implementing the rules. I look forward to seeing the Department’s response to Senator Morrissey’s request for any serious and credible fiscal analysis that was conducted in accordance with the rules’ adoption.

The final matter I want to raise and which is most instructive to this hearing on the emergency rule is New Jersey’s recent experience in adopting rules to regulate data security and privacy. Like Massachusetts, New Jersey originally proposed overly prescriptive and unworkable rules that were not consistent with federal law, that did not provide flexibility in their implementation, and that would have been unduly burdensome and costly to implement. Unlike Massachusetts to date, however, New Jersey listened to these concerns. The New Jersey administrators went back to the drawing board and substantially revised their regulations. The revised version has been

pre-proposed for comment by affected persons and the public to make sure New Jersey “gets it right” before even pursuing the official rule adoption process.

We believe that, by listening to the regulated community, New Jersey has gotten it right and we support their revised regulations. Their pre-proposed rules represent a well-reasoned, balanced approach to privacy and data security. It took New Jersey two years to get their data security regulations right (not including the actual time for implementation) and pre-proposed for comment. I respectfully submit to you that Massachusetts simply cannot get it right without first listening to and hearing the concerns of business and working together with the business community. Moreover, as indicated by New Jersey’s experience, getting it right involves a deliberative process where substance takes precedence over haste.

In Senator Morrissey’s recent letter to Secretary O’Connell, he suggested that in lieu of Massachusetts reinventing the wheel, it should be able to adopt the standards and protections used in other jurisdictions which ensure “a more seamless transaction and also data protection”. We wholeheartedly concur with Senator Morrissey. In light of the near unanimous opposition to the current form of the rules, we strongly recommend

that the Department heed Senator Morrissey's advice and consider using New Jersey's approach as its guide – incorporating a withdrawal of the current rules, engaging in a meaningful dialogue with persons subject to the rules, , re-promulgation of new rules that are both compliant with the express language of Chapter 93H and consistent with Federal law, and that appropriately balance the concerns of national and international businesses with the state's interest in protecting nonpublic personal information held by persons conducting business in the state. Additionally, this process should ensure that, upon adoption, the public is provided ample time to comply with the rules.

Thank you for your time. My industry stands ready to assist the Department in adopting rules that are effective and achieve the goals the Legislature created.



1401 H Street, NW, Washington, DC 20005-2148, USA
202/326-5800 www.ici.org

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 Massachusetts 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

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.

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

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

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 program³ – 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 the proposed 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

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.

Mr. Bryan Jamele, Legal Services Administrator
January 10, 2008
Page 5 of 5

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-Bliley 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



1401 H Street, NW, Washington, DC 20005-2148, USA
202/326-5800 www.ici.org

October 8, 2008

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

Mr. Scott Schaeffer
Office of the Massachusetts Attorney General
One Ashburton Place
Boston, MA 02108

Re: Mutual Fund Compliance with the
Standards for the Protection of
Personal Information of
Commonwealth Residents

Dear Messrs. Murray and Schaeffer:

I appreciate the time you took yesterday morning to discuss concerns of the mutual fund industry with the compliance date of the Standards for the Protection of Personal Information of Residents of the Commonwealth (the "Standards"), which were recently adopted by the Office of Consumer Affairs and Business Regulation (the "Office"). As you know, the Standards have a compliance date of January 1, 2009. For the reasons set forth below, the Investment Company Institute,¹ on behalf of the mutual fund industry, is writing to request that this extension date be postponed until January 2011. While this may seem like an unduly long extension, based upon the unique structure of our industry and our recent experience in complying with regulations of the Securities and Exchange Commission ("SEC"), we believe it will take two years for the mutual fund

¹ The Investment Company Institute is the national association of U.S. investment companies, including mutual funds, closed-end funds, exchange-traded funds (ETFs), and unit investment trusts (UITs). 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 \$12.11 trillion and serve almost 90 million shareholders.

industry to comply with the new rigorous standards. Moreover, considering the current turmoil in our financial markets, we believe this is the wrong time to impose upon the industry new rigorous regulatory requirements that will result in significant and costly burdens on the industry.² As there was no cost benefit analysis published in connection with either the proposed or adopted versions of the rule, the Office may be unaware of the significant costs and burdens that compliance with the Standards will impose on the mutual fund industry.

As a preliminary matter, the Institute presumes that, consistent with rulings of the U.S. Supreme Court under the Commerce Clause, it is not the intent of Massachusetts to impose the Standards on persons outside the boundaries of Massachusetts.³ Indeed, were Massachusetts to take the view that the Standards apply to persons outside the Commonwealth, such a view would create a real and impermissible risk of inconsistent regulations by different states. Moreover, such interpretation would seem to regulate impermissibly the conduct of Massachusetts' sister states in their treatment of information about residents of Massachusetts. For example, most every state today has established an education savings plans pursuant to Section 529 of the Internal Revenue Code. It is not unusual for residents of one state to buy another state's 529 plan. As such, it is likely that Massachusetts residents have invested in 529 plans offered by one or more of Massachusetts' sister states. Because the opening and maintenance of a 529 plan account requires the sharing of personal information, undoubtedly some, if not all, of Massachusetts' sister states are in possession of personal information relating to Massachusetts' residents. We suspect that such states would take great offense if Massachusetts took the view that the Standards apply to such states and that Massachusetts has enforcement authority over such states to the extent necessary to enforce compliance with the Standards. Because there is no carve out, in either the law enabling promulgation and adoption of the Standards or in the Standards themselves, that would relieve Massachusetts' sister states from having to comply with the Standards, we presume that it is the Commerce Clause that provides such protection and such protection has equal application to all persons located outside the Commonwealth.

Because Boston is often referred to as the home of the mutual fund industry, limiting the application of the Standards to persons within Massachusetts' boundaries will still have a major impact on the mutual fund industry. Indeed, some of the largest mutual fund companies and their service providers are domiciled in Massachusetts. It is for this reason that we strongly encourage the Office to consider how the Standards will impact mutual fund companies located in Massachusetts.

² Our members are currently in the throes of complying with a rule recently adopted by the Federal Trade Commission that has an effective date of November 1, 2008 and that requires all financial institutions, including mutual funds, to have written identity theft prevention programs in place. While both the FTC's rule and the Standards seem calculated towards the same end – protection of accountholder information to prevent identity theft – the two rules bear little resemblance to each other and, consequently, impose very different requirements on mutual funds that must comply with both. See FTC Rule 681.2.

³ See, e.g., *CTS Corp. v. Dynamics Corporation of America*, 481 U.S. 69 (1987) and *Healey et al. v. The Beer Institute et al.*, 491 U.S. 109 (1989).

THE UNIQUE STRUCTURE OF THE MUTUAL FUND INDUSTRY

Unlike other companies, mutual funds are not operating companies with employees in the traditional sense. Instead, they are externally managed and rely upon third parties or service providers to invest fund assets and carry out the fund's business activities. These service providers include, among others, the fund's:

- **Investment Adviser** – which is regulated under the Investment Advisers Act of 1940 and which manages the fund's portfolio according to the objectives and policies described in the fund's prospectus. In addition to its investment adviser, a fund may have one or more sub-advisers that are charged with managing portions of a fund's portfolio.
- **Principal Underwriter** – which is regulated under the Securities Exchange Act of 1934 and which is charged with selling the fund's shares, either directly to the public or through other firms (*e.g.*, broker-dealers). It is not uncommon for the fund's principal underwriter to enter into agreements with thousands of broker-dealers, bank trust departments, third-party administrators of pension plans, insurance companies (through variable annuity separate accounts), and others to distribute the fund's shares throughout the United States.
- **Transfer Agent** – which is regulated under the Securities Exchange Act of 1934 and which executes shareholder transactions and maintains records of transaction and other shareholder account activity.
- **Custodian** – whose activities on behalf of the mutual fund are regulated under the Investment Company Act of 1940 and who holds the fund's assets and maintains them separately to protect shareholders' interests.
- **Administrator** – which oversees the performance of the companies that provide services to the fund and ensures that the fund's operations comply with applicable federal and state law requirements.

In addition to the above, funds also utilize independent public accountants and auditors to certify the fund's financial statements and audit the fund's activities; mailing services that print and mail information to fund shareholders; banks that may be affiliated with a shareholder's account; information storage facilities (*e.g.*, Iron Mountain); information destruction services; and others.

The unique structure of mutual fund companies requires them to engage with a variety of entities in order to operate the business of a mutual fund, which includes, among other things, effecting offers and sales of the fund's shares, processing fund transactions, and maintaining records regarding the fund's operations and its compliance with federal law.

THE STANDARDS' REQUIRED CERTIFICATION

Among other issues, the Institute is particularly concerned with the provision in the Standards that requires mutual funds, as a condition to sharing information with any third-party service provider,

to “obtain from the third-party service provider a written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of [the Standards].” *See* 201 CMR 17.03(f). As a result of this provision, a mutual fund would be prohibited from sharing information – as required by federal law as necessary to process a transaction requested by a mutual fund shareholder – without having in hand a written certification from the recipient of the information that such recipient is fully compliant with the Standards. As such, before the recipient can provide such certification, it, too, must have adopted its own comprehensive information security program, including the computer system security requirements. Many such entities are likely unaware of Massachusetts’ Standards because they are not aware of Massachusetts’ assertion of jurisdiction over them through these regulations.

Of concern to the Institute is that mutual funds have only been provided approximately three months to implement a compliance information security program, including the computer security standards, and obtain all required certifications from their service providers. Based upon our experience with recent rulemaking initiatives of the SEC, we believe this compliance period is too ambitious and unrealistic. In 2004, the SEC adopted amendments to Regulation S-P, which is the regulation the SEC adopted to implement the privacy provisions of the Gramm-Leach-Bliley Act. These amendments required mutual funds and other SEC registrants to adopt policies and procedures regarding the proper disposal of consumer report information. Realizing the burdens this requirement would impose on those SEC registrants that had existing contracts with service providers for services involving the disposal or destruction of consumer report information, the SEC provided such registrants approximately eighteen months to revise their existing contracts with such service providers. *See SEC Release No. 34-50781*, 69 Fed. Regis. 71322 (Dec. 8, 2004). It bears emphasizing that this eighteen month period was necessary to implement amendments that were far more limited in their impact than the Standards in two ways. First, they impacted a far smaller universe of service providers than are impacted by the Standards; the SEC’s rule only impacted destruction services, the Standard impact every person that touches a Massachusetts resident’s personal information. Second, the SEC’s amendment only required the service provider to certify that it was properly disposing of covered information.⁴ By contrast, the Standards require *every* recipient of a Massachusetts resident’s personal information to have a rigorous information security program that complies with the Standards.

Another, more current, example of the time that may be involved in mutual funds complying with the Standards is the SEC’s 2005 adoption of Rule 22c-2 under the Investment Company Act of 1940.⁵ Rule 22c-2 required mutual funds to enter into shareholder information agreements with each of their financial intermediaries that distribute fund shares (*e.g.*, broker-dealers, bank trust

⁴ No doubt, each of the contracts mutual funds had to re-execute with those service providers covered by the SEC’s 2004 amendments will need to be revised and re-executed to accommodate the requirements of the Standards.

⁵ *See Mutual Fund Redemption Fees*, SEC Release No. IC-27255 (Feb. 28, 2006), which is available on the SEC’s website at: <http://sec.gov/rules/proposed/ic-27255.pdf>.

departments, pension plans, insurance companies, etc.). The purpose of these agreements was to enable mutual funds to have access to trading information on shareholders who hold their account through financial intermediaries to enable funds to monitor for market timing activity that violates their market timing policies. In total, the SEC provided investment companies approximately 25 months to have their agreements in place prior to the rule's compliance date. (Failure to have an agreement with an individual intermediary precluded that intermediary's ability to purchase fund shares after the rule's compliance date.) As arduous and burdensome as it was for mutual funds to obtain such agreements with each of their financial intermediaries – which numbered in the thousands for many, many funds – such burdens and ardor pale by comparison to what is entailed by the Standards because the universe of contracts that will need to be amended under the Standards to obtain the required certification will be *far more extensive* than the agreements that had to be executed under Rule 22c-2. Simply put, this process cannot be completed within three months.

Aside from the certification portion of the Standards, we believe a three month compliance period woefully underestimates the amount of time that it will take mutual funds to create, implement, and document their written information security programs. Among other things, this process will involve evaluating the totality of their “reasonably foreseeable internal and external risks,” “identifying . . . records, computing systems, and storage media . . . to determine which records contain personal information,” imposing “reasonable restrictions upon physical access to records,” acquiring or developing the full panoply of computer system security requirements imposed by the Standards, drafting the required written policies and procedures to document and govern their information security programs, testing and validating such policies and procedures, and implementing ongoing monitoring capability, each of which are requirements imposed by the Standards. Importantly, it is *not just the fund that must undertake these activities, but every entity with which the fund shares personal information*, which, as explained above, is extensive and can number in the *thousands* for an individual fund complex.

Each of the requirements in the Standards will impose extensive burdens on funds and other entities with which they share information and require the allocation of significant resources to complete. Indeed, considering the industry's vast reliance and interdependence on technology – including, for example, desk tops, laptops, websites, PDAs, telephony systems including VOIP and bluetooth, fax machines, and copiers – just conducting an inventory of all such devices and the security risks they present will be a massive undertaking. In addition, as contemplated by the “physical access” provision in the Standards, mutual funds and their service providers will also have to consider document handling and the “human” element as part of their inventory. This is an incredibly massive undertaking for the mutual fund industry and its scope – and the resources it will require – should not be underestimated.

It bears noting that the requirements imposed by the Standards will be undertaken by funds *ab initio*. This is because there is currently no requirement under federal law that requires mutual funds to have such rigorous or extensive information security programs. While the SEC, in March 2008,

Messrs. Murray and Schaeffer
October 8, 2008
Page 6 of 6

proposed information security program requirements similar to those of the Standards, such proposal has yet to be adopted.⁶ Accordingly, today, funds are not required to perform and document each of the activities that are required by the Standards. In our comment letter on the SEC's proposal, we have requested a two-year compliance period.⁷

Based upon what compliance with the undertakings will entail, and based on our experience with the time it took to implement two recent SEC rules that are not nearly as extensive in their scope and requirements as what will be required under the Standards, we respectfully request that the Office provide mutual funds ample time to comply with the revised rule's requirements. In our view, any period less than 24 month will not provide funds ample time to comply. Accordingly, we respectfully request that the compliance date for the Standards, as applied to SEC registered mutual funds and their service providers, be delayed until January 1, 2011.

We very much appreciate your consideration of this request. If you have any questions regarding it or would like additional information concerning the issues raised in this letter, please do not hesitate to contact the undersigned by phone (202-326-5825) or email (tamara@ici.org). Because time is of the essence in this matter, I look forward to your prompt response to this request.

Sincerely,



Tamara K. Salmon
Senior Associate Counsel

⁶ See *Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information*, SEC Release No. 34-57427 (Mar. 4, 2004), which is available on the SEC's website at: <http://sec.gov/rules/proposed/2008/34-57427.pdf>.

⁷ The ICI's comment letter is available on the SEC's website at: <http://sec.gov/comments/s7-06-08/s70608-22.pdf>.

**TESTIMONY OF THE INVESTMENT COMPANY INSTITUTE
BEFORE THE COMMONWEALTH OF MASSACHUSETTS
JOINT COMMITTEE ON CONSUMER PROTECTION & PROFESSIONAL LICENSURE**

My name is Tami Salmon and I am here today representing the Investment Company Institute. The Institute is the national association of the U.S. mutual fund industry. Members of the Institute operate in all 50 states, as well as internationally; they manage total assets of over \$11 trillion; and they serve almost 90 million shareholders. As regards the Commonwealth of Massachusetts, approximately half of the households here own at least one mutual fund and these shareholders account for approximately \$290 billion in mutual fund assets.

As you probably know, Boston is the birthplace of the mutual fund industry. The first mutual fund was founded here in March 1924 a few blocks from here and, today, the Commonwealth continues to be the epicenter of the industry with Massachusetts investment companies managing \$2.4 trillion in assets, or 21% of the total industry assets. Importantly, these companies are also large employers in the Commonwealth, employing over 33,000 persons, or approximately 20% of the total employees in the industry. It is because of the importance of the Commonwealth to the industry that I am here today and I very much want to thank

Chairmen Morrissey and Rodrigues and members of the Committee for both holding this hearing and permitting us to participate in it.

As a preliminary matter, I want to stress that mutual funds have long taken seriously their obligation to protect the confidentiality and integrity of non-public consumer information. This obligation derives not only from requirements imposed on us under Federal law, but on each fund's interest in protecting its brand image. Our industry depends on investors' trust to survive and an important component of that trust is protecting the confidentiality, security, and integrity of shareholders' information, regardless of where that shareholder may reside. It is for this reason that our members have spent tens of millions of dollars on their information security systems and why they continue to revise them as necessary to ensure they address new and emerging vulnerabilities and threats.

Notwithstanding that commitment to data privacy, I am here today to express the very serious concerns our members have – not with the provisions of Chapter 93H that authorized rulemaking – but with the manner and substance with which the Department of Consumer Affairs and Business Regulation undertook its rulemaking responsibility under Chapter 93H. Our concerns with the Department's resulting rules are fourfold:

- First, they appear to exceed the Department's statutory authority;
- Second, they will impede interstate commerce;
- Third, they appear to impermissibly subject the Commonwealth's sister states to the Commonwealth's regulatory requirements and enforcement authority; and
- Fourth, they are overly prescriptive, which makes them difficult to implement and, ironically, less effective.

I will briefly explain our concerns in each of these areas.

As regards the four concerns I would like to address, the first one relates to the Department's rules exceeding their authority under Chapter 93H. In granting rulemaking authority to the Department, Chapter 93H specifically required that any rules adopted by the Department "*be consistent with* the safeguards for the protection of personal information set forth in the federal regulations by which the person is regulated." Since 2000, when the SEC adopted Regulation S-P under the Gramm-Leach-Bliley Act, mutual funds have been subject to federal regulations requiring that they insure the security and confidentiality of all customer records and information; protect against any anticipated threats or hazards to such information; and protect against unauthorized access to the information that could result in any substantial harm or inconvenience to any customer.

Accordingly, we presumed that, pursuant to Chapter 93H, the federal protection accorded all mutual fund shareholders – not merely those who are resident of the Commonwealth – would suffice for purposes of complying with the Department’s rules. Unfortunately, however, this appears not to be the case because, according to the General Counsel of the Department, as used in Chapter 93H, the Department interprets the “consistent with” language to mean “not inconsistent with.” As such, so long as the Department’s rules were not “inconsistent with” any related federal rules, the Department’s could impose whatever data security requirements it deemed appropriate. I respectfully submit, however, that “consistent with” and “not inconsistent with” are two very different standards. Had the Department acted consistently with the legislative language and adopted rules that are “consistent with” the federal regulatory standards applicable to our members, I would not be before you today.

The problem with the Department interpreting “consistent with” to mean “not inconsistent with” results in the second of my four concerns – the fact that the Department’s rules will impede interstate commerce. Mutual funds are both a national and international business. As recognized by Congress in 1996 when it preempted the ability of states to regulate the operations of mutual funds, the

inconsistent actions of a single state can thwart the policies of federal regulators to impose uniform national policies on national businesses. We believe the Department's current regulations are a vivid and disturbing example of the manner in which a single state's very well-intentioned actions can have a debilitating impact on a national business.

Let me give you an example of this. Boston Financial Data Services ("BFDS"), which is located in Quincy, Massachusetts, services the accounts of more than 100 mutual fund companies. In all, they maintain close to 200 million accounts from investors all over the United States and the world. Notwithstanding BFDS' longstanding commitment to protect the data entrusted to them, under the Department's rules, BFDS now must determine which of the 200 million accounts it holds involve personal information on Commonwealth residents, and revise its systems as necessary to make sure that such accounts are protected as required by the Department's very specific requirements. But what happens if tomorrow, California, or Mississippi, or Wyoming decides that they have a better approach to securing the information on their state's residents that is in direct conflict with some of the prescriptive Massachusetts standards? The technology our members depend upon to operate, and the integrated nature of the systems throughout our industry, make it virtually impossible any mutual fund or service company like

BFDS to wrap state-specific data with state-specific requirements. This is why – as was the case with the substantive regulation of mutual funds – it is **absolutely crucial to our industry that we have one national standard governing our data security requirements.** We believe that standard should be set by the Federal government and we believe that, as enacted, Chapter 93H supports this approach to regulation. Unfortunately, as implemented, the Department's rules take a different approach.

The industry's third concern with the Department's rules is that they appear to regulate Massachusetts' sister states. While I am not here to protect and defend the rights and interests of your sister states, mutual funds will be directly affected by the resulting conflict.

Let me provide you two examples of this. Like the Massachusetts UFund 529 college savings plan, every state has a 529 plan. Members of the Institute have been retained by the various state plans to administer these plans, including investing their assets and servicing their account holders. Under the Department's regulations, before a mutual fund could provide a state information about its 529 account holders, the mutual fund would have to get a certification from the state confirming that the state is compliant with the Department's rules. Also, any

information sent to the state electronically would have to be encrypted. So what is the mutual fund to do if (1) the state refuses to sign the certification and (2) it is either unable or refuses to accept encrypted information? Similar issues will arise as the Commonwealth and its sister states continue their practice of asking mutual funds to share with them personal information on Commonwealth residents pursuant to such state's delinquent taxpayer or "deadbeat dad" laws. These are very real issues for mutual funds because of the nationwide nature of their business.

My fourth concern with the Department's rules is their overly prescriptive nature. Security experts and federal regulators – including the Department of Homeland Security – advocate so called "principles-based" regulation whereby, rather than prescribing detailed requirements, regulations impose standards on affected businesses, and leave to the business' judgment the decision of how to achieve such standards. By contrast, the Department has imposed very specific requirements that apply without regard to the nature of the business, its size and scope, its vulnerabilities, or any other relevant factors.

We submit that such a "one-size-fits-all" approach is wholly inappropriate when it comes to data security. This is because, the more standardized the security

is, the easier it is to defeat, particularly, on a large-scale basis. Moreover, however, such prescriptive requirements lock us into yesterday's security and technology, which some mutual funds and their service providers may have advanced beyond. For example, the rules require encryption of all personal information stored on laptops or other portable devices. Many of our members, however, have abandoned securing information on portable devices through encryption. Instead, they utilize "kill pills," which disable devices remotely. If a laptop is misplaced or stolen, the information stored on that laptop can be erased remotely. Under the Department's rules, however, mutual funds that have employed this more advanced technology will be required to resort once again to encrypting their information. This is but one example. Every day new and more effective security technologies are developed. We respectfully submit that, so long as rules such as the Department's prescribe very specific means of securing information, in the long run, personal information on the Commonwealth's residents will be less – not more – secure because it will be impossible for state rules to keep pace with changing technologies and emerging vulnerabilities.

Finally, I want to express our continuing concerns with the Department's overly aggressive date for complying with the rules. On Monday, September 22nd, we were informed that the Department had adopted these rules and that all persons

must be compliant by January 1, 2009. When we raised the inadequacy of this compliance period with the Department, they responded that “the mutual fund industry has now had almost 11 months’ notice” of the promulgation of the rules – which implies that we should have begun complying with the rules at the time they were proposed for comment. Not only does such a response make a mockery of the public comment process, but it evidences a fundamental misunderstanding of how businesses operate. I am not aware of any business that would expend considerable time, energy, and resources on proposed rule requirements that may or may not ever be adopted.

While we appreciate the compliance date extension the Department granted last Friday, we submit that it bears no rational relationship to the implementation process and the Department has no evidence to support why it believes one year is an appropriate extension. With respect to the May 1, 2009 extension, the Department’s press release notes that this date is consistent with a new Red Flag rule adopted by the Federal Trade Commission. However, there is no relationship between the Department’s rules and the FTC’s rule, which is far less prescriptive than the Department’s rules. Moreover, the FTC provided persons subject to its rule, which is but a small subset of persons subject to the Department’s rules, a total of 18 months to comply with it. As regards the one year extension on certain

provisions in the Department's rules, we have sound evidence that, notwithstanding our members' best efforts, which have been underway since the rules were adopted, it will take our members **no less than two years** to be compliant with such rules.

In closing, I want to express my sincere appreciation for your holding today's hearing and offering us an opportunity to express our concerns. Each of the issues I have mentioned today is a very real concern for an industry born in Boston and for which Boston today remains the epicenter. In our view, if the Department had adopted rules that were "consistent with" the Federal regulations governing the data security practices of mutual funds, I would not be here today and mutual funds and their service providers would not be dealing with each of the issues I have discussed in my testimony. On behalf of the mutual fund industry, I strongly urge this Committee to hold the Department to its authority under Chapter 93H and ensure that, for federally-regulated financial institutions, there be but one national data security standard.

Thank you for your time and I will be happy to respond to any questions at the appropriate time.



1401 H Street, NW, Washington, DC 20005-2148, USA
202/326-5800 www.ici.org

November 26, 2008

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

Re: Mutual Fund Meeting Follow-up

Dear Mr. Murray:

It was nice to finally meet you. Thank you again for the time you and Mr. Crane took to meet with me and several representatives of the Investment Company Institute¹ to discuss mutual funds' concerns with the recently adopted Standards for the Protection of Personal Information of Residents of the Commonwealth (the "rules"). As we noted during our meeting, one of the purposes of the meeting, in addition to expressing our general concerns with the rules' contents and the aggressive (and unrealistic) compliance date attached to them, was to discuss provisions of the rules that mutual funds need guidance on prior to being able to fully implement them. To address our concerns, you and Mr. Crane asked us to provide you a list of such concerns, which is the purpose of this letter. Accordingly, below is a list of the issues mutual funds have identified on which they need interpretive guidance. While Mr. Crane cautioned us against being too specific in our request for guidance, we believe that the very detailed and prescriptive nature of the rules' requirements necessitates that the Department provide us specific guidance in order for us to be able to implement the rules' requirements as written.

Before I list the issues, I want to respond to what appears to be a continuing concern of Mr. Crane. Both during our meeting and during his testimony before the November 19th hearing of the

¹ The Investment Company Institute is the national association of U.S. investment companies, including mutual funds, closed-end funds, exchange-traded funds (ETFs), and unit investment trusts (UITs). 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 \$11.2 trillion and serve almost 90 million shareholders. With respect to Massachusetts, an estimated 1.2 million, or 50% of households, own at least one mutual fund. Investment companies in Massachusetts manage approximately \$2.4 trillion in assets and employ in excess of 33,000 people.

Mr. David Murray
November 26, 2008

Joint Committee on Consumer Protection and Professional Licensure (the "Joint Committee"), he seemed most interested in what actions businesses are taking today to comply with the rules. I can assure both you and Mr. Crane that mutual funds take very seriously their duty to comply with all applicable federal and state laws and the rules thereunder governing their activities. As such, since they first became aware in September 2008 that these rules were adopted, they have been reviewing their requirements, conducting gap analysis to determine the areas they need to address, and beginning the process of implementing the rules. In other words, mutual funds are not watching the compliance date clock tick away hoping that some intervening action will alleviate their need to comply with the rules' requirements.

AREAS IN WHICH MUTUAL FUNDS NEED INTERPRETIVE GUIDANCE

Mutual funds have identified the following issues as ones on which they need interpretive guidance in order to implement fully the rules' requirements. If you have any questions concerning any of these concerns, please let me know.

I. Rule 17.02, Definitions

- A. "Personal Information" – this definition and its use in the Rules 17.03 and 17.04 raise three issues for our members:

First, if a person has an individual's name and either a Social Security number, driver's license number, state-issued identification card number, financial account number, or credit or debit card number, but no address for the individual, so the person cannot know, based on the information it possesses, whether the individual is a Massachusetts resident, what duty does the person have to determine the residence of the person to which such information relates? This issue arises, for example, in connection with the 200 million shareholder account records that Boston Financial Data Services holds on individuals from throughout the United States and the world where, for example, a person may be listed as a beneficiary on a mutual fund account with no indication as to where that beneficiary resides. Depending upon how the Department addresses this issue, the date for complying with various provisions of the rules may need to be delayed for a significant period of time to obtain any missing information.

Second, is it the Department's intention to include in the definition of "personal information" personal information that is merely returned to the person who originally shared such information? For example, assume Company A shares personal information with Company B. If Company B returns the information to Company A, must Company B have a certification (as required by Rule 17.03(f)) from Company A stating that Company A is compliant with the requirements of the Standards? This situation is very common in the mutual fund industry where a broker-dealer that accepts a mutual fund transaction forwards the shareholder's information to the mutual fund company for

processing. Once the trade is effected, the mutual fund company shares with the broker-dealer information confirming the transaction. In such instance, before the mutual fund can confirm the transaction to the shareholder's broker-dealer, must the mutual fund have in hand a certification from the broker-dealer, even if the entirety of the personal information the mutual fund provides to the broker-dealer is information the broker-dealer had originally provided to the mutual fund?

Third, what is meant by "financial account number"? As was raised during the testimony at the November 19th Joint Committee hearing on the rules, is an account number, for example, on a contract to provide janitorial or heating oil services, deemed to be a "financial account" for purposes of the rules? Or, instead, is this term intended to mean only those account numbers for an account maintained by a financial institution? The answer to this question is crucial for mutual funds to know which accounts are covered by the rules' requirements.

- B. "Person" – while this definition expressly excludes the Commonwealth and any of its subdivisions, we note there is no similar carve out for the Commonwealth's sister jurisdictions – both Federal and state. As such, it appears the intent of the Department is to subject the Commonwealth's sister states and the Federal Government (and its subdivisions) to the prescriptive requirements of the rules to the extent they own, store, or maintain personal information on a Commonwealth resident. So, for example, is it the Department's intent, as currently appears to be the case based on a plain reading of the rules, to require a sister state that requests personal information on a Commonwealth resident pursuant to its delinquent taxpayer or "deadbeat dad" statutes, to accept such information in an encrypted format as required by Rule 17.04(3)? Similarly, if one of the Commonwealth's sister states enters into a business arrangement with a mutual fund to manage or administer such state's 529 education savings plan, is it the Department's intent to require such state to agree in such contract to comply with the rules and provide a certification to such mutual fund prior to the mutual fund providing the state access to any information on accounts held by Massachusetts residents? In particular, we seek the Department's interpretation of whether the term "person" includes persons outside the Commonwealth, including Massachusetts' sister states and the Federal Government.²

II. Rule 17.03, Duty to Protect and Standards for Protecting Personal Information

- A. **Prefatory Language** – The prefatory language to Rule 17.03 raises two issues:

² To the extent the Department expresses the view that the Commerce Clause of the U.S. Constitution precludes the application of the rules to its sister states, we would be most interested in knowing the Department's views concerning whether these same restraints preclude the application of the rules to persons outside the Commonwealth that have no presence within the Commonwealth.

(1) What is meant by the phrase “reasonably consistent with industry standards”? Where is one to find what constitutes the appropriate standards for a particular person (*i.e.* a particular industry)? To our knowledge, there are no such industry standards governing the conduct of the mutual fund industry so we are uncertain as to what standards this language refers. We presume many other persons subject to the rule similarly have no such “industry standards.”

(2) The prefatory language expressly states that a program’s compliance with the regulations “shall be evaluated taking into account (i) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program, (ii) the amount of resources available to such person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information.” The prescriptive provisions of the rules, however, seem to apply without regard to any of these four factors. Accordingly, we are curious as to how the Department expects a person to take these factors into account in implementing the rules requirements and how it expects the Office of the Attorney General to consider these factors in enforcing compliance with the rules. Any insight the Department can provide on this issue is most appreciated.

- B. **Subsection 17.03(b)** – Mutual funds are confused by the phrasing of this provision. According to its language, persons subject to the rules must improve, “where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to: (i) ongoing employee (including temporary and contract) employee training; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures.” Is this provision intended to *require* that persons engage in (i), (ii), and (iii) or, instead, are these intended merely as examples of how a person might improve its current safeguards? We would appreciate the Department clarifying the meaning of this provision.
- C. **Subdivision 17.03(d)** – This provision requires persons subject to the rule to impose “disciplinary measures for violations of the comprehensive information security program rules.” Is it the intent of the Department that the disciplinary measures be specific to the security program rules or, instead, if a person has disciplinary measures for violating other operating, compliance, and/or regulatory policies and procedures, is that sufficient for purposes of complying with this provision? The answer to this question is necessary for mutual funds to know how precise their written policies and procedures pursuant to the rules must be.
- D. **Subdivision 17.03(e)** – This provision requires a person to “immediately” terminate a terminated employee’s access to records containing personal information. If a person has a process to terminate such access “as soon as reasonably practicable,” is it the

Department's intent that such a standard would comply with this requirement? If not, we would appreciate the Department defining what, in its view, "immediately" means (*e.g.*, within a certain number of hours, etc.).

- E. **Subdivision 17.03(f)** – Undoubtedly, this provision will impose great burdens on persons subject to the rules as it will require them to revisit all existing contracts with service providers and obtain the requisite certifications.³ Accordingly, it is absolutely crucial for mutual funds to know, with precision, which of their business relationships are subject to these requirements. Complicating compliance with this provision is the fact that the rules have failed to define the term "third-party service provider." Accordingly, we seek the Department's interpretation of what constitutes a "third-party service provider" as such term is used in this rule. For example, is the language in subdivision (ii) of Subdivision 17.03(f) intended to limit this subdivision application to entities with which a person has a contractual relationship (which seems to be implied by Subdivision (ii)) or, instead, is it intended to require all persons subject to the rule to have a contractual relationship with each third-party service provider? If it is the later, what constitutes a third-party service provider – for example, must consideration be paid for a person to be deemed a third-party service provider? Also, is it the Department's intent that entities such as self-regulatory organizations registered with the U.S. Securities and Exchange Commission under Section 15A of the Securities Exchange Act of 1934 be deemed third-party service providers? What about the U.S. Postal Service and overnight mail delivery services – does the Department deem them to be "third-party service providers" for purposes of these rules? As discussed above under our comments relating to the rule's definition of "person," because the Commonwealth's sister states currently fall within the definition of "person" does the Department intend for such sister states to be deemed "third-party service providers" if

³ *Cf.* Governor Patrick's Executive Order No. 504, *Order Regarding the Security and Confidentiality of Personal Information*, which was issued September 19, 2008 to implement the provisions of Chapter 93H by imposing on the Commonwealth and its subdivisions information security requirements. Though this Executive Order was issued in response to statutory authority that was substantively identical to the authority requiring the Department's rulemaking, it imposes far less onerous requirements on the Commonwealth and its subdivisions. By way of example, neither the Commonwealth nor its subdivisions are required to revise any existing contracts with third-party service providers. Instead, are only required to revise their contracts with service providers prospectively as they enter into any new contracts after January 1, 2009. Similarly, neither the Commonwealth nor its subdivisions are required to encrypt or accept encrypted data. Moreover, but for the provision relating to prospective contracts, there are no compliance dates imposed in the Executive Order, which means agencies have the luxury of complying with any of the Order's provisions at their convenience and based on their own time frame. We question why the requirements the Department imposed on the private sector are much more onerous than those imposed on the Commonwealth under the same statutory chapter. This seems particularly unjust and unfair in light of the fact of the fact that the Commonwealth is likely in possession of far more personal information than the private sector and the fact that we believe financial institutions have stronger protections for maintaining the security, integrity, and confidentiality of personal information. An example of this is the fact that some, if not all, agencies of the Commonwealth will not accept encrypted personal information from the private sector, which requires some mutual funds to unencrypt information before providing it to the Commonwealth.

they have contractual business relationships involving a person subject to the Department's rules? If not, what language within the rule excludes them from treatment as a "third-party service provider" and what other persons may be similarly excluded?⁴

Another issue raised by this provision relates to a "chain" of third-party service providers. For example, assume a resident of the Commonwealth goes to its local broker-dealer, Broker-Dealer A, to purchase a mutual fund. In order to effect the customer's order, the Broker-Dealer A shares the information with another larger broker-dealer, Broker-Dealer B, that has an omnibus trading platform. Broker-Dealer B, in turn, forwards the transaction to the mutual fund's principal underwriter (another registered broker-dealer), Broker-Dealer C, which then forwards the trade to the mutual fund's transfer agent for recordkeeping purposes. Once the trade is effected, the transfer agent issues a confirmation (including personal information), which flows to the investor via Broker-Dealers A, B, and C. This very common distribution system raises the issues of (1) which of these entities – assuming they are each unaffiliated with each other – is a third-party service provider of Broker-Dealer A? Also, which of these entities is a third-party service provider of the fund? The answers to these questions are crucial to know inasmuch as the rule prohibits the sharing of personal information with a third-party service provider without a person first having obtained a certification of compliance from such service provider. Also, in order for Broker-Dealer B to certify to Broker-Dealer A, must it either have in hand certifications from Broker-Dealer C, the fund's transfer agent, and the mutual fund or is Broker-Dealer A only required to have a certification from Broker-Dealer B? If it's the latter, must Broker-Dealer B have obtained a certification from Broker-Dealer C regarding Broker-Dealer C's compliance prior to Broker-Dealer B providing a certification to Broker-Dealer A? Needless to say, *these are very real issues for our members that reflect mutual fund distribution channels and it is necessary for us to understand how the Department intends the requirements of subsection (f) to apply in instances such as this.* While we understand, as noted above, that the Department has expressed concerns with providing specific interpretations to specific industries, it adopted very specific and prescriptive rules and because the Department is the only person in a position to explain what it intends by its prescriptive provisions, we believe it is incumbent upon the Department to provide persons subject to the rules specific guidance of its intent in adopting these rules.

⁴ The Institute was most disappointed to read in "Industries Rip New Identity Theft Protection Rules," *State House News Service* (Nov. 19, 2008) that Mr. Crane allegedly stated, in response to similar concerns I raised at the recent hearing of the Joint Committee, that our concerns are "a law school hypothetical." Not only does this statement appear wholly dismissive of what our members, representing a major Commonwealth industry, believe to be a very serious issue needing resolution, but it underestimates the seriousness with which mutual funds take their compliance obligations. We find such comments to be counterproductive to our attempts to understand the variety of issues raised by the rules in their current form in order that mutual funds may comply fully with them.

Finally, we would like the Department to clarify what, in its view, is an adequate certification for purposes of this provision. For example, if a third-party service provider certifies as follows, would the Department consider this to be a compliant certification:

On behalf of _____ [name of third-party service provider] _____, I hereby certify that, to the best of our reasonable knowledge and belief, _____ [name of third-party service provider] _____ is compliant with the requirements of the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.03 and 17.04 (the "Standards"). In the event this entity becomes aware of any noncompliance with the Standards, we agree to notify all persons to whom we have furnished this certification.

If the Department's response to each of these issues results in the rules having broader application than their language would indicate, additional compliance time may be required beyond the current extensions to accommodate such breadth.

F. **Subdivision 17.03(g)** – The language of this provision raises many concerns for mutual funds. As adopted, this provision requires limiting the person information a person obtains as well as its use and maintenance to that "necessary to accomplish the legitimate purpose *for which it is collected.*" [Emphasis added.] It is not uncommon in the financial services industry – and we presume many other industries – for information to be obtained for one purpose and utilized for a variety of other legitimate (and legally required) purposes. For example, in our industry, information is obtained to open an account so a mutual fund shareholder can purchase a mutual fund, but such information is used for a variety of other purposes – many of which are required under state or federal law⁵ – and the information is retained for extensive periods of time – often decades. We recommend that the Department clarify that this provision is not intended to limit persons retaining personal information for a variety of purposes beyond the purpose for which it may have originally been collected.

G. **Subdivision 17.03(h)** – This provision requires identification of all records used to store personal information to determine which records contain personal information. We question how the Department intends this provision to apply to recorded telephone calls, since such recordings are considered "records" as defined in Rule 17.02. In particular, what is the identifying information the Department intends to require by

⁵ Note that, by its language, this provision only speaks to maintaining information "to comply with state or federal *retention* requirements." Our members have a panoply of state and federal regulatory requirements necessitating their maintenance of personal information beyond any such "retention" requirements.

this provision with respect to recorded calls containing personal information that are maintained by person subject to the rule?

H. **Subdivisions 17.03(j) and (k)** – Each (and both) of these provisions require ongoing oversight of a person’s comprehensive information security program. We are unable to discern, however, any substantive difference between these two provisions and would appreciate the Department providing guidance regarding what substantive differences are intended by including two provisions that seemingly impose the same requirements. In the Department’s view, what is the substantive difference between these two provisions?

I. **Subdivision (l)** – This provision requires persons to document “responsive actions taken in connection with any incident involving a breach of security.” This requirement raises several issues: (1) What does the Department intend by “responsive action”? For example, if internal meetings are held to discuss a breach, are these part of the “responsive actions” that are to be documented? If not, what actions or types of actions are to be documented? (2) How detailed must such documentation be? For example, is it to list, to the extent a person is able, the personal information that was breached? (3) What is the record retention period for maintaining the required documentation? Because this would not be a required record under any applicable provision of state or federal law, we question what the Department believes to be the required retention period.

III. **Rule 17.04, Computer System Security Requirements**

A. **Subdivision (1)(ii)** – This provision requires that persons use “a reasonably secure method of assigning and selecting passwords.” We would appreciate the Department providing us examples of what it considers to be “reasonably secure methods” when it comes to assigning and selecting passwords. Also, by what standard is reasonableness, as used in this provision, to be measured?

B. **Subdivision (2)(ii)** – This provision requires the assigning of unique identifications plus passwords “to each person with computer access.” What is meant by a person “with computer access” as used in this provision? For example, if an employee has “computer access” but no access to any personal information through such access, must such employee be assigned a unique identification and password or, alternatively, consistent with the rules’ focus on personal information, is it the Department’s intent that this provision only applies to employees who have computer access to personal information?

C. **Subdivision (3)** – This provision, which requires the encryption of records, raises several issues.

First, how is this provision to be applied to businesses that provide personal information by phone to their customers or others? In particular, how is such telephonic information to be encrypted when transmitted?

Second, what is meant by “technically feasible” as used in this provision? Theoretically, everything is “technically feasible” though it may not be practically feasible or its costs may far exceed any resulting benefit. This being the case, what does the Department intend by using the phrase “technically feasible”? Also, we understand from Microsoft that some computers older than three years may lack the ability to be encrypted without crashing. In the Department’s view, would trying to encrypt an older unencryptable laptop be an example of encryption that is not “technically feasible”?

Third, what type/level of encryption is required to satisfy the requirements of this provision?

Fourth, must all “records and files containing personal information” that are transmitted be encrypted or merely the personal information in such records and files?

Fifth, rather than requiring the encryption of information that travels across public networks, this provision requires the encryption of all personal information “that will travel across public networks.” Because potentially all data could travel over a public network, is this provision intended to require the encryption of all such data or only that data that actually travels across public networks?

Sixth, the term “data” is not defined in the rules. Is this term intended to have the same meaning as “personal information”? If not, how does the Department define “data”?

- D. **Subdivision (4)** – This provision requires the “reasonable monitoring of systems for unauthorized use of or access to personal systems.” We would appreciate the Department clarifying what duty this provision requires that is not required by the provisions of subdivisions 17.03(j) and (k).
- E. **Subdivision (5)** – This provision requires the encryption of all personal information stored on personal devices. This raises two issues: First, how does the Department define “portable devices”? Second, what if a person uses security (*e.g.*, “kill pills”) that does not involve encryption? Does the Department intend by this provision requiring encryption to impose yesterday’s security on tomorrow’s devices and vulnerabilities?
- F. **Subdivision (6)**—This provision requires up-to-date firewalls and patches for personal information “on a system that is connected to the Internet.” What does the Department intend by using the phrase “connected to the Internet.” If a person has a system with both intranet and Internet access, but the files containing personal information are only available

on the intranet system, does the Department believe such system is “connected to the Internet” for purposes of this provision?

- G. **Subdivision (7)** – This provision requires “reasonably up-to-date” versions of system security software. This requirement raises several questions. First, what is meant by “reasonably up-to-date” as used in this provision? In particular, what standard does the Department intend to be used to determine reasonableness for purposes of this provision? Second, we note that this provision does not seem to be tied to any personal information files or records. Does the Department intend that the security requirements of this provision apply only to software or systems containing personal information or does it intend for it to have broader application? Third, this provision requires the use of “software that can still be supported with up-to-date patches and virus definitions.” Is it the Department’s intent to require persons to deploy all new systems if their existing systems cannot be supported with “up-to-date patches and virus definitions”?
- H. **Subdivision (8)** – This provision requires the training of employees “on the proper use of the computer security system.” We do not understand the meaning of this provision and would appreciate the Department clarifying what it means by “the proper use of the computer security system.” Perhaps if the Department could provide us an example of a “proper use of a computer security system” we might better understand the meaning of this requirement.

THE DEPARTMENT’S “SMALL BUSINESS GUIDE FOR FORMULATING A COMPREHENSIVE INFORMATION SECURITY PROGRAM”

The Department recently published “a collection of documents that focus on helping small business with the task of complying with [the rules].” These documents, which include one entitled “Small Business Guide for Formulating A Comprehensive Information Security Program,” have been posted on the Department’s website. While we commend the Department for attempting to assist persons in complying with the rules, we are puzzled by their focus on assisting “small business” inasmuch as there is nothing in the rules that distinguish the rules’ application to small businesses versus any other size business. In addition, however, we are concerned with the language of Section V of the Small Business Guide, which relates to “Internal Risks.” Our concern results from the fact that the prefatory language to this section lists “measures [that] are mandatory” under the rules. These “mandatory measures” include each of the following:

- Each employee must receive a copy of the Plan and, upon receipt “acknowledge in writing that he/she has received a copy of the Plan.”
- “There must be immediate retraining of employees on the detailed provisions of the Plan.”
- “Employment contracts must be amended immediately to require all employees to comply with the provisions of the Plan, and to prohibit any nonconforming use of person information during or after employment . . .”

- The Data Security Coordinator shall be responsible for conducting the annual review of “all security measures” “and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.”
- Requiring that a terminated employee’s “voice mail access [must] . . . be invalidated.”
- “The Data Security Coordinator shall maintain a highly secured master list of all lock combinations, passwords and keys.”⁶
- “Current employees’ user-Ids and passwords must be changed periodically.”
- Employees must be “encouraged to report any suspicious or unauthorized use of customer information.”
- Employees must be “prohibited from keeping open files containing personal information on their desks when they are not at their desks.”
- “*Each department*” must “develop rules . . . that ensure reasonable restriction upon physical access to records . . . including a written procedure that sets forth the manner in which physical access to such records *in the department* is to be restricted; and *each department* must store such records and data in locked facilities, secure storage areas or locked containers.” [Emphasis added.]
- “Re-log-in [by employees] shall be required when a computer has been inactive for more than a few minutes.”
- “Visitor access must be restricted to one entry point for each building in which personal information is stored, and visitors shall be required to present a photo ID, sign-in and wear a plainly visible “GUEST” badge or tag. Visitors shall not be permitted to visit unescorted any area within our premises that contains personal information.”

While we commend the Department for attempting to assist small businesses in complying with the rules’ requirement, we believe that any such assistance should be entirely consistent with the rules’ requirements. Instead, it appears that the Department has attempted to provide advice that would lead small businesses – or any business subject to the rules – to believe that each of the above listed requirements are imposed by the rules when, in fact, *there is nothing in the adopted rules that impose any of these requirements*. Accordingly, we strongly recommend that the Department either clarify where the rules impose each of the above “mandatory measures” or, in the alternative, revise its Guide to clarify that none of these measures are required by the rules.⁷

⁶ As an aside, security experts indicate that vesting all such security access in one person is an unsafe practice that increases an entity’s vulnerability. We therefore question why the Department believes this is a practice that should be followed by a small business or any business.

⁷ While we recognize that the Guide includes various caveats regarding the fact that “**The Guide is not a substitute for compliance with 201 CMR 17.00,**” [emphasis in original] it would seem prudent that any such Guide at least be consistent with the rules’ requirements. We believe that publishing a Guide that imposes requirements beyond those required by the rules disserves those entities that are relying upon the Department to assist them in their compliance efforts.

THE INDUSTRY'S CONTINUING CONCERNS WITH THE AGGRESSIVE COMPLIANCE DATE

In order for mutual funds to implement fully the requirements of the rules, they need resolution and guidance on each of the above discussed interpretive issues. Moreover, as noted in connection with certain of the issues discussed above, the Department's response may necessitate further extensions of the compliance date because, even with their best efforts, mutual funds will be unable to comply with the Department's current, very aggressive, compliance dates. While the Department appears to underestimate the impact of the rules – particularly the provisions of Rule 17.03(f) – on mutual funds, we have credible, objective evidence based on our implementation of federal rules that implementation will likely take *at least two years*. Notwithstanding this, according to Mr. Crane, the Department “believes,” in the absence of any credible information or evidence, that mutual funds should be able to comply with some of the rules provisions by May 1, 2009 and with the totality of the rules by January 1, 2010 and the Department has extended the compliance dates accordingly.

We strongly encourage the Department to reconsider its position on a compliance date until it obtains credible information regarding a more realistic time frame for compliance. Indeed, in the Department's announcement of the extended compliance date, it notes, in connection with the May 1, 2009 compliance date, that “businesses addressing the new FTC requirements can now address the state regulations during the same time frame.” We are quite puzzled by this statement in lieu of the fact that (1) the FTC requirement apply to a very limited subset of persons subject to the Department's rules (indeed, not all mutual funds are subject to the FTC's rules); (2) the FTC's requirements bear no resemblance to the Department's requirements; and (3) the FTC has given persons subject to its rules 18 months to comply with their requirements, which are far less rigorous and far less prescriptive than the Department's requirements and the Department, even with its extension, has only provided persons a compliance period of approximately eight months.⁸ Accordingly, we are at a loss to understand why compliance with the FTC's rules bear any relevance to compliance with the Department's rules.⁹

Obviously, time is of the essence in terms of our members getting a response from your Department in order for them to be able to implement fully the requirements of the rules. Accordingly, your prompt response to each of the issues raised in this letter is most appreciated. If you have any questions concerning any of the issues raised in this letter or need any additional information concerning these issues, please do not hesitate to contact me by phone (202-326-5825) or email

⁸ In our view, contrary to the view expressed by the Department in its recent letter to me, the compliance period only begins when a rule is adopted – not when it is proposed for comment. Indeed, for an agency to commence the running of the compliance period upon the publication of a proposed rule would appear to make a mockery of the public comment process.

⁹ The Institute has actively worked with its members on complying with the FTC's rules and we have been actively engaged with senior staff of the FTC responsible for addressing issues concerning such rules. We commend the FTC staff for working with industry to understand and address industry concerns and for extending the compliance date to ensure that persons subject to their rules have ample time to comply with them.

Mr. David Murray
November 26, 2008

(tamara@ici.org). Similarly, if you would like to discuss any of these issues with our members, we can accommodate that request as well.

Sincerely,

A handwritten signature in black ink, appearing to read "Tamara K. Salmon". The signature is fluid and cursive, with a long horizontal flourish extending to the right.

Tamara K. Salmon
Senior Associate Counsel



1401 H Street, NW, Washington, DC 20005-2148, USA
202/326-5800 www.ici.org

December 12, 2008

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

Re: Additional Information on Data Standards

Dear Mr. Murray:

I have just returned from attending the annual joint conference of the National Association of State Treasurers (NAST), National Association of Unclaimed Property Administrators (NAUPA), and the College Savings Plan Network (CSPN).¹ The Massachusetts data security standards were a topic of discussion at Committee meetings of these groups held during the conference. Indeed, state officials expressed their concerns with the Commonwealth, through its rules, seeking to impose the Commonwealth's legal requirements on the sovereignty of its sister states and indicated that they have no intent of subjecting themselves to the Commonwealth's rules. This being the case, it appears that the scenario that Mr. Crane recently referred to as "a law school hypothetical" will, in fact, be reality. As such, it is vital that, as requested in my November 28, 2008 letter to you, Commonwealth businesses be advised by your agency what they are to do when a sovereign state refuses to abide by the provisions in the rules regarding amending third-party contracts, providing certifications, encrypting information, or only accepting encrypted information when information is submitted electronically. Their unwillingness – or refusal – to abide by these requirements in the rules will result in our members' and other business' inability to be fully compliant with the rules to the extent they involve, among other things, interacting with the states as third-party vendors or transmitting personal information to such states.

¹ As you may know, these organizations are comprised of senior state officials, including State Treasurers, who are charged with administering state treasuries, 529 plans, and abandoned property laws.

Mr. David Murray
December 12, 2008
Page 2

In addition to reaffirming this concern, another issue has arisen in connection with the rules involving the administration of a decedent's estate and other legal processes. While the Federal privacy rules provide an express exception to permit the sharing of nonpublic personal information in connection with legal and regulatory processes,² the same is not true of the Massachusetts rules. Accordingly, if the executor of an estate being administered involves the transfer of personal information on a Commonwealth resident, the rules prohibit the transfer of such information until the executor of the estate is fully compliant with the Commonwealth's rules. Needless to say, the likelihood of an executor being fully compliant may be quite remote, which could result in impeding the administration of the estate. This is but yet another example of the far-reaching nature of the rules and the real world impact they will have on the ability of persons to conduct business in an unimpeded fashion. In addition to the issues I raised with you in my November 28th letter, I would appreciate your agency's guidance on issues similar to this that will result from the rules' failure to include an exemption addressing the sharing of personal information in connection with legal or regulatory proceedings.

Also, in light of the rules' fast-approaching compliance date and our members' uncertainty regarding the meaning and intent of various provisions in the rules, your prompt response to the issues raised in this letter and in my previous letter will be most appreciated.

Sincerely,

/s/

Tamara K. Salmon
Senior Association Counsel

² See, e.g., Securities and Exchange Commission Rule 248.15.



1401 H Street, NW, Washington, DC 20005-2148, USA
202/326-5800 www.ici.org

December 24, 2008

Mr. David Murray, General Counsel
Massachusetts Office of Consumer Affairs and Business Regulation
Ten park Plaza, Suite 5170
Boston, MA 02116

Re: Clarification of December 11, 2008 Letter

Dear Mr. Murray:

The Investment Company Institute appreciates your letter dated December 11, 2008, which was in response to the Institute's November 26th letter seeking guidance on various provisions in the Division's new Standards for the Protection of Personal Information of Residents of the Commonwealth (the "Standards"). We also appreciate your affirming that the form of certification we proposed in our letter would be satisfactory for purposes of complying with Section 17.03(f).

Unfortunately, most of the questions/issues we raised in our letter were either not addressed in your correspondence or addressed in a meaningful way. Some of these are listed below. Of particular concern, however, is your response relating to the required third-party certifications, which are one of the most troubling provisions in the Standards. To address concerns of our members with this requirement in Subdivision 17.03(f), the Institute's letter's stated, in relevant part, as follows (footnotes omitted; emphasis added):

Undoubtedly, this provision will impose great burdens on persons subject to the rules as it will require them to revisit all existing contracts with service providers and obtain the requisite certifications. **Accordingly, it is absolutely crucial for mutual funds to know, with precision, which of their business relationships are subject to these requirements.** Complicating compliance with this provision is the fact that the rules have failed to define the term "third-party service provider." Accordingly, we seek the Department's interpretation of what constitutes a "third-party service provider" as such term is used in this rule. For example, is the language in subdivision (ii) of Subdivision 17.03(f) intended to limit this subdivision's application to entities with which a person has a contractual relationship (which seems to be implied by Subdivision (ii)) or, instead, is it intended to require all persons subject to the rule to have a contractual relationship with each third-party service provider? If it is the later, what constitutes a

third-party service provider – for example, must consideration be paid for a person to be deemed a third-party service provider? Also, is it the Department’s intent that entities such as self-regulatory organizations registered with the U.S. Securities and Exchange Commission under Section 15A of the Securities Exchange Act of 1934 be deemed third-party service providers? What about the U.S. Postal Service and overnight mail delivery services – does the Department deem them to be “third-party service providers” for purposes of these rules? As discussed above under our comments relating to the rule’s definition of “person,” because the Commonwealth’s sister states currently fall within the definition of “person” does the Department intend for such sister states to be deemed “third-party service providers” if they have contractual business relationships involving a person subject to the Department’s rules? If not, what language within the rule excludes them from treatment as a “third-party service provider” and what other persons may be similarly excluded?

Another issued raised by this provision relates to a “chain” of third-party service providers. For example, assume a resident of the Commonwealth goes to its local broker-dealer, Broker-Dealer A, to purchase a mutual fund. In order to effect the customer’s order, the Broker-Dealer A shares the information with another larger broker-dealer, Broker-Dealer B, that has an omnibus trading platform. Broker-Dealer B, in turn, forwards the transaction to the mutual fund’s principal underwriter (another registered broker-dealer), Broker-Dealer C, which then forwards the trade to the mutual fund’s transfer agent for recordkeeping purposes. Once the trade is effected, the transfer agent issues a confirmation (including personal information), which flows to the investor via Broker-Dealers A, B, and C. This very common distribution system raises the issues of (1) which of these entities – assuming they are each unaffiliated with each other – is a third-party service provider of Broker-Dealer A? Also, which of these entities is a third-party service provider of the fund? **The answers to these questions are crucial to know inasmuch as the rule prohibits the sharing of personal information with a third-party service provider without a person first having obtain a certification of compliance from such service provider.** Also, in order for Broker-Dealer B to certify to Broker-Dealer A, must it either have in hand certifications from Broker-Dealer C, the fund’s transfer agent, and the mutual fund or is Broker-Dealer A only required to have a certification from Broker-Dealer B? If it’s the later, must Broker-Dealer B have obtained a certification from Broker-Dealer C regarding Broker-Dealer C’s compliance prior to Broker-Dealer B providing a certification to Broker-Dealer A? *Needless to say, these are very real issues for our members that reflect mutual fund distribution channels and it is necessary for us to understand how the Department intends the requirements of subsection (f) to apply in instances such as this.* While we understand, as noted above, that the Department has expressed concerns with providing specific interpretations to specific industries, it adopted very specific and prescriptive rules and because the Department is the only person in a position to explain what it intends by its prescriptive provisions, we believe it is incumbent upon the Department to provide persons subject to the rules specific guidance of its intent in adopting these rules.

In response, to the above, your letter merely states as follows:

Regarding 201 CMR 17.03(f), a 'third-party service provider' refers to any person or entity that provides a service to the principal to whom the Massachusetts resident delivered his/her personal information. No useful purpose would be served by trying to formulate a definition that will capture every kind of relationship between the recipient to whom a Massachusetts resident delivers his/her personal information and any other person or entity whom that recipient engages to transport, maintain, process, etc., that information; especially so, since third-party service providers are very well known in the mutual fund industry.

Quite candidly, I have no idea what this answer means. It seems to introduce some new concepts into 17.03(f) that we are at a loss to understand. For example, the first sentence seems to somewhat narrow the scope of 17.03(f) by implying that certifications need only be obtained from those third-parties that provide a service directly to the original recipient of the information. Is this, in fact, the Division's intent? Similarly, the second sentence, too, seems to limit the meaning of "third-party service provider," though it is unclear how such term is being limited. It begins by trying to narrow the scope of this term to those persons where a "useful purpose" would be served by including them in the rule. However, we are at a loss to understand who is supposed to make the determination regarding which third-party service providers satisfy this standard and which do not. Indeed, we note that the regulation itself provides no such "useful purpose" standard so what would be the basis for a person relying on such a standard?

Most puzzling to us is the statement in the last sentence that "third-party service providers are very well known in the mutual fund industry." While it is true that, as externally-managed entities, mutual funds must rely on a panoply of service providers to operate, that operating structure provides us no insight into how the Commonwealth interprets the term "third-party service provider" for purposes of the Standards – which was why we raised the issue in our November 26th letter. Indeed, if anything, your response seems to muddy the water even further by introducing the concepts of the person to whom a Commonwealth resident delivers information, reading into the Standards a new "useful purpose" test, and referencing the "very well known" third-party service providers in the mutual fund industry. Accordingly, once again, we are asking you to clarify with more precision, and consistent with the language of Section 17.03 and the Standards, the meaning of the term "third-party service provider." It would be most helpful to us if, in addition to making general statements regarding this term, you address the specific instances raised in our November 26th letter so we can understand, for purposes of our industry, what this term means.

In addition to the issue of third-party service providers, your letter failed to address each of the following issues raised in the Institute's November 26th letter:

- Whether, if a business maintains an individual's name and social security/account number, there is a duty to determine the state of residence of such person in order to determine whether the individual is a Commonwealth resident;
- Whether personal information merely returned to a person requires a certification from such person prior to being able to return it;
- What is meant by "financial account number;"
- Whether the term "person" includes states other than Massachusetts.
- The document retention period for the documentation of responsive actions taken in connection with breaches;
- Where in the Standards the scalability required by the authorizing statute are incorporated;
- What constitutes "technically feasible" encryption;
- What electronically transmitted information must be encrypted;
- The meaning of "data," as used in the Standards and its relationship to the meaning of "personal information;"
- The meaning of "portable devices;"
- What systems are considered "connected to the Internet" for purposes of the Standards' requirements relating to firewalls and patches;
- What is meant by "reasonably up-to-date" versions of system security software; and
- What would constitute training "on the proper use of the computer security system."

In addition, in my supplemental letter to you dated December 12, 2008, I raised the additional issues of:

- How persons subject to the Standards are expected to address the unwillingness – or refusal – of the Commonwealth's sister states to abide by the Standards' requirements in Section 17.03(f) relating to contractual provisions and certifications;
- The ability to share personal information with estate administrators and others pursuant to legal proceedings when such sharing may result in the violation of one or more provisions of the Standards.

We would very much appreciate your response to these concerns as well as those concerns raised in my November 26th letter that remain unaddressed. Moreover, in light of the Standards' fast-approaching compliance date and our members' uncertainty regarding these issues, your prompt response to this letter will be most appreciated.

Sincerely,

/s/

Tamara K. Salmon
Senior Associate Counsel



Garry B. Watzke, Esq.
Senior Vice President
Legal and Business Development
Corporate Offices
745 Atlantic Avenue
Boston, MA 02111
Tel: 617-535-4702
Fax: 617-451-0409
E-Mail: garry.watzke@ironmountain.com

January 21, 2009

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

RE: Massachusetts Regulation 201 CMR 17.00, Standards for the
Protection of Personal Information of Residents of the Commonwealth

Gentlemen:

Iron Mountain Incorporated is a Boston-based provider of information storage and management services. We provide storage and management services for information on paper and electronic media in most states of the United States and many other countries.

One of our business lines consists of providing secure off-site storage for back-up and archival computer tapes, cartridges and cassettes. In the off-site storage of backup and archival media, the media is physically transported from customers' data centers to our secure storage facilities, and then re-transported from our storage facilities to customers' data centers on a pre-scheduled date or when the media is required for business purposes.

201 CMR 17.04(5) requires that companies that own, store, license or manage personal information of Massachusetts residents encrypt such information on laptops and other portable devices. We are uncertain as to the meaning of the phrase "other portable devices" in this context. Specifically, does the phrase "other portable devices" include backup and archival tapes, cassettes and cartridges, thereby requiring that it be encrypted? If the OCABR interprets the phrase to have such meaning, it would have a very disruptive effect on many companies in the United States and other countries, because encryption of backup and archival tapes would be quite expensive and adversely affect the utility of backup tapes.

We appreciate your prompt attention to this question.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Garry B. Watzke".

Garry B. Watzke

From: Jamele, Bryan (EOHED)
Sent: Thursday, January 22, 2009 5:02 PM
To: Murray, David (SCA)
Cc: Crane, Dan (SCA); McCollum, Ryan (EOHED)
Subject: FW: Oppose Data Security Changes!

-----Original Message-----

From: Moore, Richard (SEN) [mailto:Richard.Moore@state.ma.us]
Sent: Thursday, January 22, 2009 4:06 PM
To: Jamele, Bryan (SEA)
Subject: FW: Oppose Data Security Changes!

Please register this letter from Mr. VanderBaan with regard to comments about the Draft 201 CMR 17.00 Senator Richard T. Moore

-----Original Message-----

From: mail.relay@mailmanager.net [mailto:mail.relay@mailmanager.net] On Behalf Of James VanderBaan
Sent: Thursday, January 22, 2009 3:41 PM
To: The Honorable Richard T. Moore
Subject: Oppose Data Security Changes!

James VanderBaan
17 Carr St.
Sutton, MA 01590-2344

January 22, 2009

The Honorable Richard T. Moore
Massachusetts Senate
Massachusetts State Senate
Boston, MA 02133

Dear Senator Moore:

As a small business owner I ask that you take into consideration the time and expense these modified data security regulations will have on my business.

My business is facing many financial challenges this year, and a new mandate from the state would only make things harder for me to keep all my employees. The cost of doing business is already too high!

Please oppose and delay the proposed data security regulations in Massachusetts. Think of how this will affect the thousands of small businesses across the state that are already dealing with a sputtering economy.

Sincerely,

James VanderBaan

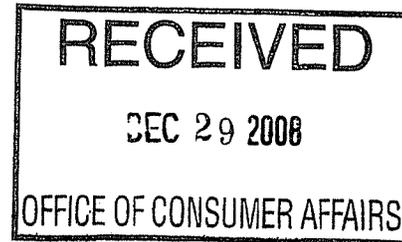
US Legal

John Hancock Life Insurance Company
Post Office Box 111
Boston, Massachusetts 02117
(617) 572-0862
Fax: (617) 572-1565
E-mail: Curtis_Morrison@manulifeusa.com

Curtis Morrison
Vice President and Counsel

December 12, 2008

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



RE: MA Privacy Regs

Dear Mr. Murray:

Thank you for the opportunity to comment on Regulation 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth. The comments expressed herein are submitted on behalf of the John Hancock Life Insurance Company (USA) and its family of financial services companies.

Section 2(a) of Chapter 93H of the Massachusetts General Laws requires the Office of Consumer Affairs and Business Regulation (OCABR) to adopt regulations for the protection of personal information relating to residents of the Commonwealth. Section 2(a) goes on to require that those regulations "...shall be consistent with the safeguards...set forth in federal regulations by which..." a covered person or entity "...is regulated..."

Despite the clear language of 93H, some of the regulations adopted by OCABR (201 CMR 17.00) are not consistent with existing federal privacy regulations applicable to financial services companies and their customers. Furthermore, in a time of severe economic challenges for most businesses, the OCABR regulations mandate covered persons to adhere to requirements that will be costly to implement, but will not provide additional protections for Massachusetts' residents.

Support for the above conclusion is contained in Section 17.03 (f) of the OCABR regulations. Under Section 17.03 (f) "persons" who provide personal information to third party service providers must first do three things: determine that selected providers are capable of maintaining appropriate safeguards for that information (due diligence); contractually require providers to maintain such safeguards; and—prior to permitting them access to personal information—require that they execute written certifications of their compliance with the OCABR regulations.

The first two of those requirements are consistent with "best practices," existing federal privacy regulations governing financial services companies, and clearly both provide

protection for personal information. Financial services companies like John Hancock are (under federal privacy regulations) already required to comply with those requirements.

However, under the OCABR regulations, "persons" sharing personal information, even under long standing contracts with reputable and fully vetted service providers, will have to incur the difficulty and expense of obtaining certifications before being able to continue to share personal information with those providers after January 1, 2010. Such certifications provide no additional protections for Massachusetts' residents. Rather, protection is effectively established as a result of appropriate due diligence and the inclusion of strong privacy protection provisions within a given vendor's contract.

Mandating a superfluous and costly certification requirement makes no sense when the aforementioned due diligence and contractual provision requirements have been fully satisfied. By insisting that certifications be in place for existing vendor contracts before personal information can be shared after January 1, 2010, the Commonwealth potentially undermines existing vendor relations that are already governed by contracts with strong privacy protections; and it unintentionally puts at a competitive disadvantage financial services companies with customers who are Massachusetts residents, when compared to those companies that either have no such residents as customers or are effectively beyond the Commonwealth's enforcement powers. As such, John Hancock respectfully requests that the third party service provider certification requirement be rescinded.

In the alternative, John Hancock submits that a more reasoned approach for incorporating certifications within Massachusetts' regulatory process would be to only require them on a prospective basis: after January 1, 2010, all newly contracted third party service providers who are provided personal information would be required to complete written certifications. Making certifications a prospective requirement appears to be the approach taken by Section 9 of Massachusetts' Executive Order No. 504, wherein on September 19, 2008, state agencies were required—on a prospective basis—to obtain certifications of compliance with both the Order and 93H from all vendors who receive personal information relating to Massachusetts residents. Clearly what is reasonable for the Commonwealth regarding procedures to protect personal information should also be reasonable for all other persons covered by the OCABR regulations.

John Hancock thanks you for the opportunity to be heard on this important issue. Please feel free to contact the undersigned if you need additional information relating to this letter.

Yours truly,



Curtis Morrison
Vice President and Counsel

Testimony for the Joint Committee on Consumer Protection & Professional Licensure by Steven Michalove, Principal Security Strategist at Microsoft

Informational Hearing on November 19th relative to the content and implantation of proposed regulation 210 CMR 17.00 Standards for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts.

I am Steven Michalove, principal security strategist at Microsoft, and I want to thank you for the opportunity to testify today.

To start, Microsoft would like to commend the Joint Committee on Consumer Protection, and the Patrick Administration, especially Undersecretary Dan Crane and Attorney General Martha Coakley, for their efforts to ensure the sensitive personal information of Massachusetts residents is protected from identity theft and other online threats. This is a common goal that the public and private sectors share equally.

At Microsoft, protecting computer users against risks in the "Internet age" , including the risks of identity theft, is a top priority. We are committed to making the investments necessary in the operation of our own business and to deliver technologies that enhance security for computer users around the world. At the same time, we recognize that security is an extremely complex equation, and that it is important that all stakeholders -- industry, the public sector, and users alike -- work together and be thoughtful about how to fight online crime, including identity theft.

There is clearly a role for well-crafted and meaningful legislation and regulations to protect against the risks of identity theft. However, as a technologist, I have concerns about certain aspects of the regulations promulgated by the Office of Consumer Affairs and Business Regulation. Specifically, I would like to address the encryption-related requirements in the regulations. While encryption can and does play a role in building a well-rounded set of controls to protect sensitive information, it is no silver bullet. The industry is in a constant "arms race" against those with nefarious intent. Encryption may or may not be the best use of scarce resources in addressing these threats over time. These requirements are technically problematic, potentially extremely costly, and would have serious unintended consequences for businesses and organizations of all sizes.

17.04: Computer System Security Requirements (3) To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly

With respect to encryption of all transmitted records that will travel across public networks and, to a certain extent, for all data to be transmitted wirelessly, there are significant barriers to implementing a technical solution for small and large businesses alike. While the challenges are different for small businesses compared to large businesses, there are some common elements that make deployment

difficult. These include the challenge of interoperability, the availability of mature technology, and the resources that it would take to implement a common solution. Let me say a few words on each of these challenges:

First, the chief challenge in scrambling information crossing public networks is one of Interoperability. Data that is scrambled by the sending party must be unscrambled by the receiving party. Interoperability is critical -- sender and receiver must agree on confidential keys, sharing of those keys and decryption methods ahead of time. PKI (Public Key Infrastructure) is the technologist's dream state solving this "shared secrets" problem but the end users "nightmare" -- expensive to build and hard to use. It takes a great deal of technical talent to design, implement and operate. Massachusetts's own Government Taskforce Force found PKI so complicated that it recommended creation of a PKI Task Force (http://www.mass.gov/Aitd/docs/online_gov_task_force_rpt.pdf). Nevertheless, many large enterprises (and agencies) -- but not small businesses -- do operate such PKI infrastructures. Like the Commonwealth, they often outsource these certificate services (http://www.mass.gov/Aitd/docs/operations_managed_services.rtf) and they most often limited to SSL Web certificates. If two enterprises do happen to operate PKI infrastructures that do issue encryption capable certificates for email, the users must be knowledgeable enough exchange certificates across the enterprises prior to the information exchange. These systems are not "natively" interoperable.

Second, the interoperability challenge also is exacerbated by the issue of availability. While encryption technologies may be "technically feasible" they are not readily available, and are certainly not widely deployed or used by businesses in Massachusetts or, for that matter, elsewhere in the United States. For example, email encryption technologies such as PGP (Pretty Good Privacy), S/MIME (Secure/Multipurpose Internet Mail Extensions) and DRM (Digital Rights Management) exist and provide varying types of protection against unauthorized viewing. However, there is no one standard among these technologies, they may be superseded by other technologies, and they are not universally used. While there are a few service providers inside the financial services industry that provide a secure email service (e.g. SWIFT http://www.swift.com/index.cfm?item_id=60759 and Citigroup <http://www.citi.com/citi/citizen/privacy/email.htm>) these systems are not compatible with one another and depend upon proprietary technologies or certificates. In short, they are not interoperable.

Third, even if a standard form of encryption technology necessary to fulfill compliance were commonly accepted and readily available in the marketplace (which it is not), it would take a significant amount of time and financial resources for businesses to acquire and deploy the necessary hardware, software or services, and to pay for the related services to implement "encryption" for all relevant electronic transmissions. Small businesses have a gap in skills and financial resources needed to implement the provisions of the regulation whilst large enterprises will have the challenge of scale. To deploy this to large numbers of users takes significant investment and years of deployment effort. While some countries, most notably Denmark, have overcome this through the deployment of national Public Key Infrastructures, and then widely implemented them in the public domain and in eGovernment, ; this is not an option currently available in the Commonwealth nor in the US Federal domain. A good source of additional obstacles can be found at: <http://www.oasis-open.org/committees/pki/pkiactionplan.pdf> by the Organization for the Advancement of Structured Information Standards

17.04: Computer System Security Requirements (5) Encryption of all personal information stored on laptops or other portable devices

Information on laptops or other portable devices is clearly a potential security risk. Indeed, many current industry surveys indicate that over 50% of data breaches are caused by lost or stolen devices. Encrypting the data on these devices is one way to significantly mitigate this risk. But it is not the only one. Cyber security should be viewed holistically, and not limited by definition to any one technological requirement. I would like to discuss some of the challenges to encryption to demonstrate why the government, by regulation, should not dictate any one technological solution.

As a general matter, the very flexibility and decentralized mobile nature of these devices that makes them so useful also makes it costly and slow for organizations to deploy and enforce encryption as a method of protecting the data stored on the devices. The basic underlying challenge of shared secrets is the same with this scenario as above with a few notable differences. Normally, the key is created by software, and then encrypted with a secret (passwords, PIN's, finger print, etc.). In an institution or corporation, secondary access to the data must be provided to authorized third parties (like law enforcement, corporate fraud investigators, or network administrators) via a secure key escrow infrastructure. So not only does the enterprise need to deploy encryption technologies, it must also design and implement a key escrow infrastructure.

Laptops

With respect to laptops, there are common obstacles to deploying data encryption on laptops owned by small and large organizations. In general, the industry practice is to encrypt the whole data volume and not just individual files. This obscures the data both in its primary location as well as in temporary files, meaning the end-users do not need to think about what and where to encrypt. It is also hard to know what is sensitive and what is not, so it is often easier to encrypt everything compared to having to decide file by file. While there are various hardware (disk drive) and software solutions available – there is no clear or emerging standard. Currently, most new laptops shipped from factories do not include full disk encryption as a standard hardware nor software feature. These systems must be retrofitted and converted.

Conversion of existing systems is both time consuming and labor intensive. With current hardware, it takes about 1 minute per Gigabyte of disk size to convert a system. For a 120Gbyte hard drive this will mean a minimum of 2 hours for the conversion. New systems are starting to ship with 300Gbyte drives which will more than double the encryption time. As drive sizes increase, so do encryption times. So not only must technicians likely handle each system in order to install the necessary software the actual setup can take hours for each computer. Additionally, anecdotal evidence indicates that about 10% of laptop drives over 3 years old cannot survive the encryption process due to the stress placed on the hardware. While the drive will have failed sometime in the future, encryption acts as an early detector forcing disc replacement, causing potential data loss unless proper backup procedures are in place and then another round of encryption on the new drive. Small and large organizations alike must pay for the encryption solution and then provide both the labor and skills needed to convert existing systems. For enterprises with hundreds of thousands of systems, this can take years to deploy and can be quite expensive (often exceeding \$200 in direct and indirect cost per PC).

Larger enterprises also face the creation of a monitoring and compliance framework to enforce the progress of deployment and ongoing compliance. Since solutions have not become standards, this will mean significant investment in custom inventory and management tools. Additionally, large organizations will also have to develop technologies and processes for key escrow and drive recovery. This includes everything from password resets to dealing with litigation eDiscovery requests. Since the technology is so immature, the burden for deployment is high and requires a high level of specialized technical skills to build custom solutions.

Portable Devices

The portable device scenario is even more challenging and the technology less mature. We like to call these roaming devices since they tend to be used on one PC and then plugged into another PC. The huge variety of devices and media from thumb-drives, cameras and music players to memory chips and cell phones makes encryption difficult. These technologies often do not work when using the memory device across platforms, for example, when using a memory card in both your PC and in a camera. As always interoperability can be a major barrier when dealing with devices and software from different manufacturers.

- If a software solution is chosen, that software must run on all of the systems the media may roam to. If it requires a license, the user must purchase that software and make it available. For some platforms like camera's and cell phones, no solution may be available.
- The burden of key escrow must also be considered with roaming devices in the for large businesses and institutions.
- Interoperability across time is an issue. If you encrypt a USB Thumb drive this year, will you still be able to read it in one year's time? The solution you may have been relying on may now be technically obsolete or the licenses may have lapsed.
- Many devices break when encrypted. If you plug your MP3 player into your PC and then encrypt its drive it will most likely no longer function as a music player. There is no standard way to encrypt such small devices and it is often not possible at all. Interoperability is often lost when encrypted.
- One of the viable options available to users is prevent the data from getting onto devices in the first place. For example, make the drive "read only" if not encrypted (the user is unable to save files to them from the PC. This remains a technical challenge with a variety of emerging solutions.

Conclusion

Encryption is certainly one of many tools that can help protect the security of personal information. However, it is not the only one and the law should not mandate such a limiting and restrictive requirement on businesses. Moreover, as noted, there is no reasonable means by which businesses – small or large – could comply with this strict encryption requirement in the near future. The technical

and deployment barriers are significant and will take years to develop and deploy. Industry is committed to the goal of protecting the security of personal information and understanding how to reasonably protect such information. Unfortunately, current encryption technologies are not sufficiently advanced or widely deployed to make this possible on a comprehensive or reasonably affordable basis for several years. Ubiquitous use encryption is just not possible with current technologies.

A better approach would be to provide businesses and individuals — which are in the best position to understand the particular security measures that are best suited to the different types of storage and transmission devices they maintain — the discretion to implement the most appropriate technologies and procedures for their respective environments. This flexibility is also critical because cyber security, of which encryption-related technologies are simply one tool, is an ever-changing technological challenge. It is a constant arms race against a variety of threats. Security measures are constantly evolving and improving as technology advances and engineers respond to evolving threats to information security. By imposing an inflexible encryption requirement, the Commonwealth would risk having its own regulations become obsolete and potentially limiting on businesses and organizations.

LIFE INSURANCE ASSOCIATION
OF MASSACHUSETTS

501 Boylston Street, Boston, Massachusetts 02116-3700
Phone: (617) 375-9200 Fax: (617) 375-1029

January 16, 2009

Mr. Daniel C. Crane
Director
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116

Dear Director Crane:

I am writing on behalf of the Life Insurance Association of Massachusetts regarding proposed 201 CMR 17.00, concerning the protection of personal information of residents of the commonwealth. LIAM is a trade association representing thirteen leading life, health, disability income and long term care insurers licensed to do business in the Commonwealth. Nine of these companies are domiciled in Massachusetts.

LIAM and its member companies have long been supporters of consumers' privacy rights. Insurance companies are financial institutions which are subject to the federal Gramm Leach Bliley Act, including its safeguarding provisions. We comply with GLB as well as the privacy laws of the states in which we do business, including M.G.L. c. 175I, the Insurance Information and Privacy Protection Act.

M.G.L. Chapter 93H requires the Department of Consumer Affairs and Business Regulation to adopt regulations which are consistent with the federal safeguarding regulations under the Gramm Leach Bliley Act. Unfortunately, the proposed regulation, as drafted, is inconsistent with all of the federal safeguarding regulations promulgated pursuant to GLB, as well as with the Model developed by the National Association of Insurance Commissioners, also pursuant to GLB.

We respectfully recommend the Office of Consumer Affairs and Business Regulation deem persons who maintain procedures for protection of personal information pursuant to GLB and the safeguarding rules thereunder be considered to be in compliance with the 201 CMR 17.00. This tracks the approach taken in Ch. 93H with regard to security breaches which states that "a

person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs...."

If compliance with federal rules is not deemed to be compliance with 201 CMR 17.00, we believe that companies should be given more time to comply. While we appreciate the extension dates the Office has proposed, we believe that they do not afford enough time for companies to come into full compliance with the regulation. We respectfully recommend that the compliance dates be further extended to at least June 1, 2010.

We also respectfully recommend that you eliminate the requirement for third party certification and make the contracting requirement effective for new and renewed contracts only. The regulation's contract and written certification provisions are duplicative, unnecessary, and unduly burdensome.

In addition, we are hopeful that the Office of Consumer Affairs and Business Regulation will clarify that, if the requirement is not eliminated, certification from third party vendors is required only once as well as provide a definition for the term "portable device."

We would be pleased to provide you with any further information that you may find helpful as you consider this important issue.

Sincerely,



Andrew J. Calamare
President and Chief Executive Officer
Life Insurance Association of Massachusetts

From: bounce@bounce.votervoice.net on behalf of Kim Burdon [kburdon@madixinc.com]
Sent: Tuesday, January 13, 2009 12:37 PM
To: General Counsel David Murray
Subject: Change Mass. Data Regulations

General Counsel Murray:

As an employer in the North Brookfield, MA with 55 of employees, I am very concerned about the mandates currently included in 201 CMR 17.00. As written, these regulations set a difficult course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth.

My facility is the smallest division of our parent company. We were acquired in 2003 and have been struggling with getting and maintaining work ever since largely due to our higher cost structure for utilities and labor. Our capabilities are not unique in our company, therefore we have to compensate for our higher cost structure with improved efficiency and innovation.

To this point, we have weathered the recent storms of increased costs (health care) and higher taxes. However, the costs and the changes in business practices that appear to be required by the current version of the personal data law and regulations are extremely painful.

The pain arises because our company stores our records, along with the records of the other 95% of company employees, in a common database. Therefore, any changes required in Massachusetts impact that entire database and the procedures required to manage these data corporate wide.

We are diligently pursuing the process of evaluating the methods and costs required to comply. However, even at this point, I don't believe that we feel that we are fully confident we know those requirements.

Please reconsider breaking new ground in this area. These regulations appear to be demonstrably more aggressive than other states, the health care industry or the federal government. By taking this approach it becomes that much harder to argue to maintain Massachusetts operations. This would take the products we have earned the right to produce by our efforts and innovation and send them, and our Massachusetts jobs, elsewhere.

Sincerely,

Kim Burdon
9 Blueberry Ln
Sturbridge, MA 01566



January 16, 2009

Daniel C. Crane, Undersecretary
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116

Re: Amendments to 201 CMR 17.00 – Standards for the Protection of Personal Information of Residents of the Commonwealth

Dear Undersecretary Crane:

I am writing on behalf of the Massachusetts Association of Health Plans (MAHP), which represents 12 health plans that provide coverage to 2.3 million Massachusetts residents, with regard to 201 CMR 17.00. Our members place a high priority on protecting the personal information of individuals they serve. While we are supportive of your efforts to institute measures to protect Massachusetts residents from the risk of identity theft, we are very concerned that sections 17.03 and 17.04 of the regulation assert greater jurisdiction over health plans and other entities that comply with federal requirements regarding security breaches than Chapter 93H, *Security Breaches*, created by Chapter 82 of the Acts of 2007, allows. We believe that requiring federally-compliant organizations such as health plans to provide additional verification and documentation would be time consuming to implement and impose unnecessary administrative requirements, increasing the cost of health care with little or no value to the consumer.

Section 2 of Chapter 93H requires that regulations adopted by OCABR “be consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated.” In addition, Section 5 of Chapter 93H requires persons (defined as natural persons, corporations, partnerships, associations or other legal entities) or agencies to comply with “any applicable general or special law or federal law regarding the protection and privacy of personal information; **provided however, a person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter** (emphasis added)...” Section 5 then continues to state the specific actions, including notices to affected Massachusetts residents and to the Attorney General and the director of the office of consumer affairs and business regulation, that the person must still meet. If the person fails to comply with any federal law, rule, or other applicable guidelines or guidance regarding security breaches, the person becomes subject to all the requirements of Chapter 93H.

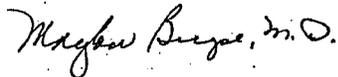
Under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, health plans already are required to have in place extensive measures to safeguard residents' protected health information, which would encompass personal information as defined under the regulations. Our recommendation is to add a separate section after sections 17.03 and 17.04 that incorporates the language from Sections 2 and 5 of Chapter 93H, including the deeming language and the

notice requirements in the event of a security breach, so that it will be clear that organizations that already meet federal and industry standards, including health plans that have implemented HIPAA requirements, are deemed to be in compliance with the regulations.

For example, 201 CMR 17.03(f), which deals with verification of third-party service providers, requires entities to take reasonable steps to verify that third party suppliers have the capability to protect information to which they have access. The section also requires that anyone permitting such access must obtain written certification that a third-party service provider has a written, comprehensive information security program. Consistent with Sections 2 and 5 of Chapter 93H, we believe, a HIPAA-compliant business associate agreement, or when appropriate, a written confirmation that a supplier is a HIPAA-covered entity should be recognized as satisfying the requirements of 17.03(f). Requiring additional verification and documentation would be time consuming to implement and impose unnecessary administrative requirements, increasing the cost of health care with little or no value to the consumer.

We appreciate the opportunity to offer comment and would be happy to talk with you or a member of your staff in more detail.

Sincerely,

A handwritten signature in cursive script that reads "Marylou Buyse, M.D.".

Marylou Buyse, M.D.
President

Massachusetts Association of Insurance Agents

Professionalism Through Independence

info@massagent.com
massagent.com®

January 16, 2009

STATEMENT OF MASSACHUSETTS ASSOCIATION OF INSURANCE AGENTS BEFORE THE OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION IN CONNECTION WITH THE PROMULGATION OF AMENDMENTS TO REGULATION 201 CMR 17.00 STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH.

Good afternoon Undersecretary Crane. My name is Daniel J. Foley, Jr., and I am Vice President of Government Affairs and General Counsel for the Massachusetts Association of Insurance Agents (MAIA). On behalf of the Massachusetts Association of Insurance Agents (MAIA), a statewide trade association that represents 1600 independent insurance agencies, I would like to express our serious concerns with the provisions of the regulation 201 CMR 17.00, and the devastating financial impact that the regulation's provisions will have upon our member agencies. Although the effective date of the regulation has been extended until May 1, 2009, this extended time is still too short for insurance agencies to fully comply.



91 Cedar Street, Milford, MA 01757
TEL (508) 634-2900 • (800) 972-9312 • FAX (508) 634-2933
Francis A. Mancini, Esq., President & CEO



Page 2.

We urge the Patrick Administration to engage in a rigorous stakeholder analysis, and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 with the Department, Attorney General, regulated community and elected officials, to re-issue an entire set of rules by May 1, 2009, with the implementation of the rules over a two-year period.

Protecting a person's "personal information" as defined in the regulation is very important, and is something that MAIA and all of its member independent insurance agencies take very seriously. However, we believe that there has to be a reasonable balance between protecting a person's identity and the legal requirements imposed upon the business community in order to assure that an individual's personal information is protected from security breaches. As currently written, 201 CMR 17.00 goes beyond the legislature's intent, and mandates specific technologies, creates redundant and confusing rules, and does not hold public agencies to the standards of the private sector. These requirements and standards go beyond any existing or emerging federal privacy standards.

The standards being imposed upon every business in Massachusetts that possesses "personal information" of a Massachusetts resident will be especially devastating on the 1600 member insurance agencies of MAIA. Granted there are large insurance agencies that may well be able to comply with the regulation, but the majority of MAIA members are truly "small businesses." We have found that in a recent study that our Association commissioned to measure the impact that independent insurance agencies have on the

economy in Massachusetts, the average size agency employs seven employees, with approximately 85% of the agencies having five or fewer employees. These agencies will not be able to commit the necessary financial resources, both in personnel and money, to comply with the requirements by May 1, 2009. Compliance needs to be based upon resources available, and needs to be flexible for small businesses. The current regulation lacks flexibility. A “one size fits all” approach without regard to the nature of the business or its resources is inappropriate.

The promulgation and implementation of these specific regulations are in sharp contrast with other states, and especially other Massachusetts state agencies that routinely engage in collaborative discussions with the regulated communities. The state of New Jersey recognized the need for a vigorous stakeholder analysis. Currently, the State of New Jersey is currently in a two-year process just to promulgate a “pre-proposal” of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposed after determining in April 2008 to reconsider, and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey’s new pre-regulations do not provide similar time, clarity, recognition of federal regulations, nor do they recognize the significant technological, legal, operational challenges or the significant investments and human talent that many persons and small firms must now face.

As a member of the Business Coalition for Data Security, you have seen the list of issues and solutions identified by the business community in a letter sent to you. As I've stated earlier, independent insurance agencies will not be able to comply with the provisions of these regulations by May 1, 2009, and the financial burden placed upon our members specifically and small businesses generally, will be devastating, especially in light of today's economy. So the issue of **TIMING** is of great concern to MAIA and its members, and we support and urge the Administration to adopt the suggestions made by the Business Coalition relative to a phased-in implementation of the rules over a two-year period.

The issues of **CONSISTENCY** and **CONTRACT PROVISIONS** and **WRITTEN CERTIFICATION** for third-party service providers are of particular concern to independent insurance agencies. With respect to consistency, the current regulations go far beyond what the ID theft law requires. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents. MAIA's members conduct business with clients and insurance carriers across the country, and it is very important that everyone is on the same page regarding the privacy and data security laws.

The **CONTRACT** and **WRITTEN CERTIFICATION PROVISIONS** for third-party service providers are duplicative, confusing and unnecessary. Again, we support the recommendations of the Business Coalition that contractual language should be used and not certification, and then on a going-forward basis when contracts with third parties are newly created or renewed.

As for **MANDATORY ENCRYPTION**, this is not mandated in the law and its prescriptive nature negates the reasonableness standard within the statute. A principle or standard should be used allowing the regulated community to assure our outcome, rather than complying with a single command and control technology. This requirement will prove very costly in terms of money and personnel to independent insurance agencies, as I have indicated in previous communications with your office.

The **INVENTORY** requirement will be very costly and time-consuming as set forth in the regulation. MAIA supports the recommendations of the Business Coalition for Data Security, whereby a more meaningful approach would be to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. This approach would be similar to what is required in other federal and state contexts.

On a final point, the **PUBLIC SECTOR**, the state agencies, need to be held to exactly to the same standards as the private sector. Personal data is regularly shared with public entities, and is a source of significant data breaches.

Page 6

Secretary Daniel O'Connell was recently quoted in the Boston Globe where he said that his agency will spend less energy trying to hire out of state businesses to Massachusetts, and more time trying to help those already here to weather the tough times. If he means what he says, then given the financial crisis that we are facing in the Commonwealth, now is not the time to be imposing additional financial burdens on small businesses.

Again, on behalf of the independent insurance agencies across the Commonwealth, we urge the Patrick Administration to engage in a rigorous stakeholder analysis with your department, the Attorney General, the regulated community and elected officials, and reissue an entire set of rules by May 1, 2009 with implementation carried out over a two-year period.

Thank you for your consideration of any recommendations and giving me the opportunity to provide comments at today's hearing.

**Statement of David E. Floreen, Senior Vice President
Massachusetts Bankers Association
Regarding 201 CMR 17.00 Standards for the Protection of
Personal Information of Massachusetts Residents
Office of Consumer Affairs and Business Regulation
January 16, 2009**

Undersecretary Crane, General Counsel Murray, I am David Floreen, Senior Vice President of the Massachusetts Bankers Association and appear this afternoon on behalf of our nearly 200 member banks doing business across the Commonwealth. Our banks range from among the smallest (less than \$30 million in assets, to the largest \$1 trillion). I appreciate the opportunity to offer these comments regarding the new regulation 201 CMR 17.00, MGL Ch. 93H: Standards for the Protection of Personal Information of Massachusetts Residents (“the Rule”) issued by the Office of Consumer Affairs and Business Regulation (OCABR). The Rule is now slated to take effect on May 1, 2009.

At the outset, we want to express our industry’s longstanding commitment to ensuring the safety and security of its customers’ and employees’ personal information. Our members continually strive to enhance data security measures and regularly train their staffs on appropriate data security policies and procedures. We also want to acknowledge and express our appreciation to the Office of Consumer Affairs in delaying the effective date of the initial rule from January 1 until May 1 to allow banks and other businesses more time to prepare to implement the rule. More importantly, we would encourage OCABR to give serious consideration to modifying portions of the rule that raise major questions regarding the ability of banks and businesses to comply with certain provisions regardless of the timetable. The balance of my remarks focuses on our industry’s strong recommendation that the regulations must be revised and the effective date delayed to avoid significant unnecessary expense and confusion in the marketplace.

Since the initial regulation was released in late September 2008, the Massachusetts Bankers Association and its member banks have devoted considerable resources toward carefully assessing and evaluating the language and intent of the Rule. As the banking community more deeply analyzed the language and assessed the scope and effects of the Rule, it became extremely clear that it would have been nearly impossible for Massachusetts banks of any size to meet the January 1, 2009 compliance date. We applaud the decision by OCABR to delay the effective date for four months.

Our concerns today focus on the practical and pragmatic issues member banks have identified as they examine these newly-required due diligence, policies, procedures and compliance certifications that must be addressed and put in place by May 1, 2009.

While some of the numerous requirements contained in the Rule are not far beyond what Massachusetts banks already do to protect customer information under Title V of the Gramm-Leach-Bliley Act (GLBA) and its implementing rules, regulations and guidance, we are concerned that the Rule is overly specific and prescriptive in mandating what every Massachusetts business, inclusive of banks, must do to comply and goes to a level of detail that many businesses, large and small, financial or otherwise will struggle to meet.

For example, most banks already have comprehensive data security policies in place that are designed to detect and prevent data breaches. The focus of these policies is on risk-based parameters, not compliance with specific technical requirements. The current financial

environment has significantly eroded the ability of many businesses to fund all but the most essential services, and the regulations in their present form mandate new compliance that Massachusetts businesses, including banks, cannot and do not need in order to adequately protect personal information. We remain steadfast in the position that the clear intent of the legislature in adopting section 2 of Chapter 93H was to ensure that Massachusetts rules would be consistent with those already mandated by federal law or regulation, to the extent that an industry was subject to such rules. Clearly, the banking industry has been subject to extensive federal data security rules and guidance for several years and we believe that the proposed Rule does not follow the legislative mandate.

The following is a partial list of provisions in the Rule that exceed existing federal guidelines under GLBA or create significant compliance challenges or costs for all Massachusetts banks:

Third Party Vendor Certification:

Without question, the mandate to secure third party certification of all vendors by May 1, 2009 remains the most difficult provision. The Rule mandates that *before* an institution allows a service provider to access personal information, it must conduct due diligence to ascertain the vendor can actually safeguard the information in practice. This would require a complete re-run of every bank's vendors through its vendor risk management program at much higher, if not at the highest levels of risk and review. Once that review is complete, a bank then must request and secure from the affected vendors a written compliance certification stating the service provider has a written information security plan and a program in place that complies with the Rules. This vendor process would most likely be followed with requests to fund the vendors' efforts and/or requests for relaxed service level agreements and new pricing terms.

In essence, all banks face a massive vendor contract remediation project; each certification will be open to legal drafting interpretation and result in a required legal review as new terms and conditions are added. While the four month extension provides more time to conduct this process, given the very difficult economic situation and the intense pressure to control costs, imposing this mandate at this time is deeply troublesome. Furthermore, many third-party contracts have cancellation clauses requiring advance notice of termination and significant penalties for early termination.

If a vendor fails or is unwilling to provide a certification, and we are now learning that an increasing number of vendors, particularly those outside Massachusetts have indicated that they will not sign a written certification as currently required, a bank would have to invoke the clause, and then seek a new vendor, if in fact a suitable one was both available and capable of providing the scope and service quality that the bank expects. Many vendors executed service agreements prior to promulgation of the Rule. Choosing a new vendor is a process that takes many months and potentially forcing that process in this economic environment is ill-advised. In addition, some of the banks' core processors may not comply with the state's requirements. In those instances, entire systems and business platforms might have to be scrapped at enormous costs to the institutions.

Collection of the "Minimum Amount Necessary":

Collecting the minimum amount of personal information necessary to accomplish the legitimate purpose for which it was collected and retaining such information for the minimum time necessary to accomplish such purpose is a new heightened standard in records retention and

management. As written and understood by the industry, banks and other businesses must review all application intake points of contact and ensure that they are only collecting the minimum amount of information necessary to accomplish such (banking) purposes. This is a complex and sophisticated assessment of information that may not be covered by a standard industry practice or measurement across all industries.

Inventory of All Hard Copy and Electronic Records:

The Rule essentially requires that banks inventory all records to identify those records containing personal information. Conducting such an inventory will require banks to decide whether they can separate records in electronic or in other format, containing personal data from those that do not, or whether the business must treat all information as personal information.

Remote Access:

This requirement mandates that all affected businesses must develop security policies to determine whether such employees may keep, access, or transport data containing personal information off-premises. In turn, this forces human resource departments to work with all business functions as well as corporate officers to create new policies and procedures around remote access. For many banks and businesses, the previous compliance date of January 1, 2009 could have crippled all business functions that use remote access. The extension to May 1, and in some cases, January 1, 2010 is a welcome positive development which needs more refinement to incorporate the real world use of today's and tomorrow's personal electronic devices.

Costs of Encryption:

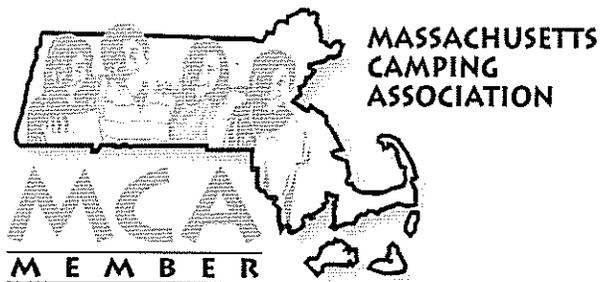
Under the Rule, banks and all businesses will have to encrypt personal information stored on laptops or other portable devices; is transmitted over wireless systems; and (to the extent feasible) it travels across public networks. Banks interact with their customers and counter-parties in highly secure environments and are required to maintain multiple levels of authentication. While banks are moving rather rapidly toward encrypting all personal information, the budgets for 2009 are challenged to provide sufficient funding for this considerable expense due to competing regulatory initiatives. This concern extends to bank vendors since they must certify compliance with such a mandate while providing service at current costs.

Conclusion:

It is important to note that the Rule was promulgated on September 24, 2008 allowing only 99 days until the initial mandatory compliance date of January 1, 2009. While some suggested that businesses had 11 months to comply, no business will invest limited resources to prepare for implementation of a regulation until it is promulgated in final form. It should be noted that the state of New Jersey has taken two years to develop now pre-proposed rules to implement a similar statute and the current proposal is notably more flexible than what is currently proposed in Massachusetts.

As promulgated, the Rule presents significant fiscal, operational and training obstacles for Massachusetts banks and businesses to meet even by May 1, 2009. We look forward to working with the Office of Consumer Affairs and strongly urge your office to reassess portions of the Rule to more appropriately reflect the legislative intent.

Thank you for considering the views of all 200 Massachusetts banks on this critical issue.



January 21, 2009

Daniel Crane, Undersecretary
Office of Consumer Affairs and Business Regulation
Ten Park Plaza, Suite 5170
Boston, MA 02116

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

Dear Undersecretary Crane:

I am writing this letter to share our perspective and concerns as they relate to the draft "Standards for the Protection of Personal Information of Residents of the Commonwealth" (201 CMR 17.00).

MCA represents the organized camps of Massachusetts. We are a group of 80 Day and Resident Camp Professionals organized in the 1970s to monitor and address regulatory issues and safety standards for the more than 1400 camping programs licensed in the state, one of the largest concentrations in New England.

While we are concerned that our many small camps will be forced to absorb another financial burden in the required encryption standards, our most significant concern is to maintain online access to the processing and delivery of Criminal Offender Record Information (CORI reports) from the Criminal History Systems Board (CHSB).

After the November 19th public hearing, we contacted the CHSB to inform them that during the hearing it was stated that the new identity theft law applied to government as well as private businesses. It is our understanding the EOPS is looking into this issue as well as CHSB but to date we have not received any confirmation that the online system will be seamlessly maintained.

Each year between the months of April and June, the CHSB processes tens of thousands of CORI reports for summer camps. Chapter 385 of the Acts of 2002 mandates that operators of camps are required to run CORI checks (which includes conviction and non-conviction data, plus pending cases), as well as their juvenile record on all potential employees and volunteers. Department of Public Health regulations also require that CORI checks be performed.

We are very concerned is that 201 CMR 17.00 may force a suspension of our online access to CORI's. This would create a major hardship on camps and could create a backlog that makes it difficult for some camps to open on time.

On behalf of the Massachusetts Camping Association, I respectfully request that these concerns be addressed prior to the implementation of final regulations.

We appreciate the opportunity to comment on this issue and would welcome the opportunity to meet with you or a member of your staff, if needed.

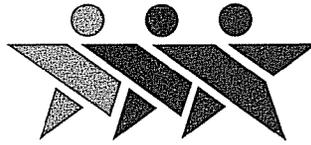
Please feel free to contact me at 508-362-3798 or will@campwk.com.

Best regards,

A handwritten signature in cursive script that reads "Will" followed by a simple smiley face drawing consisting of a circle with two dots for eyes and a curved line for a mouth.

Will Rubenstein
MCA President

CC: Daniel O'Connell, Secretary of Housing and Economic Development
One Ashburton Place, Room 2101, Boston, MA 02108



MASSACHUSETTS CREDIT UNION LEAGUE, INC.
OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION
PUBLIC HEARING
JANUARY 16, 2009

STATEMENT RELATIVE TO

**STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF
RESIDENTS OF THE COMMONWEALTH**

The Massachusetts Credit Union League, Inc. ("League") is the state credit union trade association serving 208 federally and state-chartered credit unions that are cooperatively owned by 2.4 million consumers as members and operating as part of the Credit Union National Association ("CUNA"). On behalf of the Massachusetts credit union movement, the League offers the following comments relative to the amendments to 201 C.M.R. 17.00, *Standards for the Protection of Personal Information of Residents of the Commonwealth*.

The League believes that the issue of data breaches and their potential harmful and long term impact on the residents of Massachusetts is one of the most important challenges facing us. The efforts of the Patrick Administration and the Office of Consumer Affairs and Business Regulation ("Consumer Affairs") in prioritizing this issue and in promulgating the rules, which are the first state regulatory rules of its kind across the country, is commended. The League also appreciates the efforts of Consumer Affairs in extending the general compliance date to May 1, 2009 and to January 1, 2010 for obtaining certification from third party service providers and for encrypting portable devices other than laptops through the promulgation of emergency regulations. 201 C.M.R. 17.03 (f); 201 C.M.R. 17.04 (5).

Massachusetts credit unions believe that the protection of personal financial information of members is paramount and a key component of our mission of providing the highest service to members. State and federally-chartered credit unions operating in the Commonwealth continue to be amongst the first respondents to reissue plastic card access devices in circumstances of fraud or information compromises at our own cost as a business decision to protect consumers.

The priority concerns of the Massachusetts credit union movement with the regulation focuses on two major areas: One area, which is the primary subject of the public hearing, is the deadline for compliance. The other area relates to the statutory provisions mandating that the rules be consistent with federal safeguarding of information regulations. M.G.L. c. 93H, s. 5 (applicability of federal laws). This issue was also highlighted in the League's oral and written testimony on the subject presented to Consumer Affairs on January 11, 2008.

With respect to the consistency with federal provisions, all Massachusetts credit unions are governed by the rules and regulations of the National Credit Union Administration ("NCUA") relative to the safeguarding of member information. 12 C.F.R. Part 748. In 2001, the NCUA promulgated amendments to existing security rules as were required by and to be consistent with the privacy provisions of the federal Gramm-Leach Bliley Act ("GLB").

The rule requires that a credit union's security program include features to ensure the safety and confidentiality of member's records, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or inconvenience to a member.

Credit unions must also disclose their policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information as part of the initial and annual privacy notices that are sent to members.

To assess risk to member information, credit unions must:

- identify foreseeable internal and external threats that could result in unauthorized use, alteration, or destruction of member information or information systems;
- assess the potential damage of these threats, considering the sensitivity of the member information; and
- assess the sufficiency of policies, procedures, information systems, and other arrangements in place to control risks.

To manage and control risk, each credit union should:

- Design the information security program to control risk, after considering the sensitivity of the information, as well as the complexity and scope of the credit union's activities.

The credit unions must consider the following security measures and adopt the ones that are appropriate:

- Access controls on member information, including controls to prevent pretext calling, which is when unauthorized individuals seek to obtain information by fraudulent means;
- Access restrictions at physical locations that contain member information;
- Encryption of electronic information;

- Procedures designed to ensure that information system modifications are consistent with the credit union's information security program;
 - Dual controls procedures, segregation of duties, and background checks for employees who have responsibilities for, or have access to, member information;
 - Monitoring procedures to detect actual and attempted attacks on information systems;
 - Response programs that specify actions to be taken when the credit union suspects or detects unauthorized access to information systems, including reports to regulatory and law enforcement agencies; and
 - Measures to protect against loss of member information due to potential environmental hazards.
- Train staff to implement the information security program.
 - Regularly test the information security program. The frequency and nature of the tests should be determined by the credit union's risk assessment. Tests should be conducted or reviewed by independent third parties or staff that is independent of those who develop or maintain the security programs.

With regard to overseeing outsourcing arrangements with service providers, each credit union must:

- Exercise due diligence in selecting service providers.
- Require service providers by contract to implement appropriate measures designed to meet the objectives of the rules.

Standards for the Protection of Personal Information

January 16, 2009

Page 5

- If indicated by the credit union's risk assessment, monitor the service providers to confirm that they have implemented the appropriate measures. As part of this monitoring, the credit union should review audits, summaries of test results, or other equivalent evaluations.

The regulations include a two-year grandfather clause with regard to agreements with service providers. With regard to subservicers, credit unions will not have the same level of responsibility, although each credit union must determine that the servicer has adequate controls to ensure that the subservicer will protect member information, consistent with the objectives of the rules.

The regulations also include the following standards:

- Each credit union should adjust its information security programs in light of relevant changes in technology, the sensitivity of member information, internal or external threats to the information, and the credit union's own changing business relationships.
- Each credit union should provide an annual report to the board or the appropriate committee of the board. This report should describe the overall status of the information security program and the credit union's compliance with the rules.

In light of these provisions, it remains the position of the League that the NCUA regulations are risk-based, comprehensive and substantially similar to the Commonwealth's regulatory provisions. Moreover, the League believes that support for such a safe harbor is clear in the governing statutory provisions which provide for express compliance for entities who "maintain procedures for responding to a breach of security pursuant to federal laws." M.G.L. c. 93H, s.5.

As a result, the League urges Consumer Affairs to reconsider the existing regulations and clarify that entities found to be in compliance with GLB and other comparable federal regulatory provisions are expressly in compliance with the provisions of 201 C.M.R. 17.00 et. seq.

Other concerns of the League relate to the requirements of a written third party certification. Credit unions, especially the over 50 smaller credit unions under \$5 million dollars in assets, are experiencing a large administrative burden in using their small voice and limited resources to ensure vendor compliance beyond compliance with existing contractual provisions, if such contractual provisions are even contained in older agreements.

With respect to the effective date, the League urges Consumer Affairs to further extend the compliance date through 2010 to ensure that all organizations have the requisite time to comply with the diverse provisions. Such an extension is important to credit unions, particularly if the substantive portions of the regulations remain unchanged.

The League appreciates the opportunity to offer these comments and respectfully requests your favorable consideration of the comments set forth in this Statement.

MASSACHUSETTS
HIGHTECHNOLOGYCOUNCIL

TESTIMONY

**Office of Consumer Affairs and Business Regulation
201 CMR 17.00**

January 16, 2009

**Christopher R. Anderson, President,
Massachusetts High Technology Council, Inc.**

Thank you for the opportunity to present testimony on this important issue. The Massachusetts High Technology Council was formed in 1977 by high tech CEOs whose mission was to help make Massachusetts the most competitive state in which to create, operate, and expand high tech businesses. That remains our mission today. Council members employ hundreds of thousands of skilled workers in all of Massachusetts's key technology sectors, including computer hardware, life sciences, software, medical products, defense technology, semiconductor, and telecommunications. Our board includes the executive leadership of tech employers such as Analog Devices, Boston Scientific, Dynamics Research, PricewaterhouseCoopers, and Vertex.

On behalf of the CEO members of the Massachusetts High Technology Council I would like to express significant concerns regarding several requirements of 201 CMR 17.00. Despite the sound intentions of these regulations to protect personal information and strengthen data privacy, there are unintended consequences that would be crippling to the Massachusetts economy and would unnecessarily put our businesses at a competitive disadvantage.

We strongly support the effort to more closely examine the necessity, timeline and effect of these regulations in full and ask for an open and collaborative public/private process to re-issue an entire set of rules by May 1, 2009, allowing for a two year period within which to implement the revised regulations

The Council joins a broad coalition of businesses from all sectors in asking for additional time, consistency and clarity from the administration with regards to these important regulations. The Council asks that you examine the following issues:

Timeline: We recommend a wholesale review with key stakeholders by May 1, 2009 followed by a two year implementation period.

Consistency and Competitiveness: The regulations require "safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations." Over-regulation in Massachusetts is damaging when global competitors are able to operate under a safe but less stultifying and costly business environment.

- over -

*Dedicated to Growth...
Committed to Action*

The Council maintains that requiring certification of third party vendors and mandatory encryption is duplicative, cost-prohibitive and unnecessary. We strongly recommend the results based industry standard that requires contract provisions between private and public sector entities.

Additionally, mandating encryption and prescribing a technology standard ensures an undue cost burden and limits technological enhancement of current practices. It would essentially freeze in time the current industry standard thereby providing criminals a static model to infiltrate and impede technological innovations that drive our economy and improve consumer safety.

The business community, public sector and citizens of the Commonwealth have a shared need to protect personal information and enforce data privacy laws. We ask that in weighing the best interests of all, that you extend the information gathering conversation and adoption date so that no unintentional harm or duplicative cost burden is levied in the spirit of good governing. The complexity of this issue merits a process wherein the right course is taken initially, so that mistakes may be averted and the appropriate measure of regulation be adopted for the safety and well being of Massachusetts citizens and businesses.



January 21, 2009

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

RE: 201 CMR 17.00, Relative to the Protection of Personal Information

Dear Undersecretary Crane:

On behalf of the over 250 trucking company members and the tens of thousands of individuals employed by members of the Massachusetts Motor Transportation Association (MMTA), I am writing relative to the promulgation of regulations contained in 201 CMR 17.00, *et. seq.*. As currently drafted, the requirements imposed by 201 CMR 17.00, *et. seq.*, will harm the trucking industry – particularly small to medium sized companies who cannot afford to invest in the contemplated encryption technologies nor the additional expense associated with the contractual certification of third party vendors. Accordingly, the MMTA respectfully requests your office rescind the current regulations and, as done in other states, re-issue regulations after a more comprehensive review and implementation period.

At the outset, the MMTA endorses the concerns raised in the letter from the coalition of over 40 concerned businesses and associations who have expressed practical and legal problems with the provisions of 201 CMR 17.00, *et. seq.*. That letter, which reflects the views of a wide spectrum of industries throughout the Commonwealth, cannot understate the impacts these regulations will have on the Commonwealth's employers and, subsequently, employees. Given the existing protections on the federal and state level, these regulations appear to be too broad and ill-defined.

Notwithstanding Commerce Clause concerns about regulating non-Commonwealth domiciled trucking companies, the MMTA would also like to raise another specific concern to the trucking industry. As you know, federal law has preemption over state law where Congress has expressed a clear and manifest purpose in regulating a specific industry. Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 230 (1947). Here, Congress has quite clearly chosen to regulate states' abilities to regulate the trucking industry and the transportation of property. In particular, federal law prohibits a state from enacting or enforcing "a law or regulation or other provision having the force or effect related to the price, route or service of any motor carrier or any motor carrier, broker or freight forwarder with respect to the transportation of property." 49 U.S.C. § 1450(c)(1). Moreover, direct freight shippers, such as Federal Express ("FedEx") and United Parcel Service ("UPS"), are also governed by a similar provision governing direct air carriers. 49 U.S.C. §4173(b)(4). (i.e. Federal Aviation Administration Authorization Act of 1994 forbids States to "enact or enforce a law . . . related to a price, route, or service of any motor carrier," 49 U. S. C. §14501(c)(1), see also §41713(b)(4)(a)). Accordingly, any state law or regulation that conflicts with the Supremacy Clause of the United States Constitution is null and void. Maryland v. Louisiana, 451 U.S. 725, 746 (1981).

The proposed regulations require in 201 CMR 17.03(f) that every security program:

(f) Tak[e] reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information, including (i) selecting and retaining service providers that are capable of maintaining safeguards for personal information; and (ii) **contractually requiring service providers to maintain such safeguards.** Prior to permitting third-party service providers access to personal information, **the person permitting such access shall obtain from the third-party service provider a written certification** that such service provider has a written, comprehensive information security program that is in compliance with the provisions of these regulations. (emphasis added)

Trucking companies are dually impacted by this regulation both as a third party vendor to businesses or individuals they transport for and as an entity regulated directly by the regulations due to its very nature of collecting information. (Note: the role of owner-operators within the industry even makes the trucking company, itself, responsible for the owner-operator (i.e. third party vendor)). Without overstating the obvious, the requirement to contract and provide written certification directly affects the “price” for providing the transportation of goods throughout the Commonwealth. At a minimum, businesses will require trucking companies to contract and certify that the trucking company’s security program meets vague standards that may or may not be acceptable under the regulations. As a result, the trucking company will be required to adapt to any number of different security schematics – meaning the trucking company will bear a direct cost which will directly affect the price of transporting goods. Moreover, the requirement to provide “encryption” on all devices storing personal information creates an impact on trucking companies’ ability to provide their “service” without undue burden. (*See* encryption requirement under 201 CMR 17.04(3)).

As you may know, the United States Supreme Court recently held that the State of Maine could not implement a provision of a law governing the delivery of tobacco products which would have adversely affected trucking companies’ ability to establish “price, route or service”. Rowe, Attorney General of the State of Maine v. New Hampshire Motor Transport Association, et. al., 552 U.S. ___, No.06-457, (February 20, 2008). In deciding the case, the Court relied on the decision in Morales v. Trans World Airlines, Inc., 504 U.S. 374, 378 (1992), stating, in part:

In Morales, the Court determined: (1) that “[s]tate enforcement actions *having a connection with, or reference to*” carrier “‘rates, routes, or services’ are pre-empted,” 504 U. S., at 384 (emphasis added); (2) that such pre-emption may occur even if a state law’s effect on rates, routes or services “is only indirect,” *id.*, at 386 (internal quotation marks omitted); (3) that, in respect to pre-emption, it makes no difference whether a state law is “consistent” or “inconsistent” with federal regulation, *id.*, at 386–387 (emphasis deleted); and (4) that pre-emption occurs at least where state laws have a “significant impact” related to Congress’ deregulatory and pre-emption-related objectives, *id.*, at 390. The Court described Congress’ overarching goal as helping assure transportation rates, routes, and services that reflect “maximum reliance on competitive market forces,”

thereby stimulating “efficiency, innovation, and low prices,” as well as “variety” and “quality.” *Id.*, at 378 (internal quotation marks omitted). Morales held that, given these principles, federal law pre-empts States from enforcing their consumer-fraud statutes against deceptive airline-fare advertisements. *Id.*, at 391. See American Airlines, Inc. v. Wolens, 513 U. S. 219, 226–228 (1995) (federal law pre-empts application of a State’s general consumer-protection statute to an airline’s frequent flyer program). Rowe, 552 U.S. __ (2008), pp.4-5.

In supporting the trucking associations’ assertions in *Rowe*, the Court further held that “the effect of the [Maine] regulation is that carriers will have to offer tobacco delivery services that differ significantly from those that, in the absence of the regulation, the market might dictate. . .[i]f federal law pre-empts state efforts to regulate, and consequently to affect, the advertising *about* carrier rates and services at issue in Morales, it must pre-empt Maine’s efforts to regulate carrier delivery services themselves.” Rowe, 552 U.S. __ (February 20, 2008), pp.6.

In this case, the Commonwealth is attempting to dictate how trucking companies must go about their business – whether in contracting and certification or the use of encrypted technology. There is a direct connection to “price and service” when requiring trucking companies to engage in the certain proscribed activities contained in the regulations. Both measures will lead to increased costs, directly affecting the price of transporting goods. As well, both measures will affect the way in which trucking companies do business, thereby directly affecting the “service” of transporting goods. In the absence of this regulation, it is not likely that trucking companies – particularly small sized companies – would necessarily contract for service in this manner under a market driven system as Congress originally contemplated. See Rowe, 552 U.S. __ (2008), pp.7. (“[T]o insist that the carriers provide a special checking system would allow other States to do the same. And to interpret the federal law to permit these, and similar, state requirements could easily lead to a patchwork of state service-determining laws, rules, and regulations. That state regulatory patchwork is inconsistent with Congress’ major legislative effort to leave such decisions, where federally unregulated, to the competitive marketplace.”)

With the above concerns in mind and recognizing the good intention of these efforts to protect individuals’ personal information, the MMTA respectfully requests that your office rescind the current regulations in light of the issues raised above. That said, the MMTA would welcome the opportunity to work with your office and other interested parties to ensure subsequent regulations do not potentially violate federal law. If you have any questions or concerns, please do not hesitate to contact either Anne Lynch, Executive Director of the MMTA, or me at (617) 695-3512. On behalf of the over 250 trucking company members and their employees, we appreciate your consideration of this testimony.

Sincerely,



Mark K. Molloy, Esq.
Legislative and Regulatory Counsel

Cc: Honorable Michael Morrissey, Senate Chair
Honorable Michael Rodrigues, House Chair
Joint Committee on Consumer Affairs and Professional Licensure



January 16, 2009

Daniel C. Crane, Undersecretary
David A. Murray, General Counsel
Massachusetts Office of Consumer Affairs and Business Regulation
10 Park Plaza -- Suite 5170
Boston, MA 02116

RE: Testimony for the Joint Committee on Consumer Protection and Professional Licensure Regarding the Promulgation and Implementation of 201 CMR 17.00, Standards for the Protection of Personal Information of Residents of the Commonwealth

On behalf of the Mass Senior Care Association (Mass Senior Care), which represents over 500 nursing facilities, assisted living residences and continuing care retirement communities employing 50,000 people, we are submitting these written comments on the Office of Consumer Affairs and Business Regulation's (OCABR's) amendments to 201 CMR 17.00, Standards for the Protection of Personal Information of Residents of the Commonwealth. While we appreciate the Administration's delay in the effective date of these regulations, we would respectfully request that OCABR *further* defer implementation until it can fully identify, analyze, address and resolve the numerous questions and concerns raised by the current regulations as drafted.

While Mass Senior Care is committed to protecting the privacy and security of personal data, we are very concerned that the scope and complexity of OCABR's new regulations may impose mandates that are neither technically nor economically feasible for our members at this time. As a member of the Data Regulations Business Coalition, we support the view that the Administration continue to work the Associated Industries of Massachusetts (AIM) and other business and stakeholder groups, the Office of the Attorney General and legal privacy experts during this process to ensure promulgation of regulations that protect consumer privacy and are more readily understandable and feasible for organizations to successfully implement. Specifically, the long term care nursing home community has the following concerns:

- **Dissemination of information** – We know that many long term care facilities are unaware of and/or do not understand the new regulations, and the requirements that they will impose on their operations. Our membership includes both small, independent facilities with minimal administrative staff as well as a substantial number of larger companies with multiple facilities whose corporate parent may conduct business in multiple states – the complexity of the new regulations and the related costs pose distinct compliance challenges to all of our members. While Mass Senior Care has alerted its

membership that the agency has promulgated new privacy regulations, we believe a more comprehensive public outreach and education effort by the administration is necessary to secure greater stakeholder input as well as ensure full understanding and compliance.

- **Federal standards** – It is our understanding that the privacy regulations go beyond established federal standards contained in Gramm-Leach-Bliley, and HIPAA. Companies subject to those federal regulations will still have to develop comprehensive information security program (CISP) written plans, designate employees to run them and several other specific compliance issues. We are concerned about the process and timeliness of securing a mandated certification of compliance from all of the many vendors, both local and out of state, that our members rely on to provide services to support our residents and operations. We are also concerned that the regulations require a separate and unique data breach notification to affected consumers, which will significantly affect companies conducting business in multiple states.

We appreciate the opportunity to provide written testimony for your consideration. Please do not hesitate to contact me if we may provide additional information.

Sincerely,



Abraham E. Morse
President



44 Winter St., 4th Fl.
Boston, MA 02108

www.masspirg.org (617) 292-4800 (ph)
info@masspirg.org (617) 292-8057 (fx)

To: Director Dan Crane of the Office of Consumer Affairs and Business Regulation
Fr: Eric Bourassa, MASSPIRG Consumer Advocate
Re: Testimony with regards to data security regulation implementation
Date: January 20, 2009

MASSPIRG is a non-profit, non-partisan public interest organization with approximately 40,000 members across the Commonwealth. MASSPIRG was involved in the passage of legislation to create safeguards to protect consumer information from security breaches.

MASSPIRG supports the proposal to delay the implementation of the data security regulations so that businesses and other entities can take appropriate steps to comply with the new law.

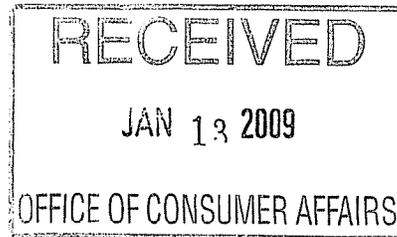
However, the law must not be delayed further. Protecting consumer information is critically important in preventing identity fraud and identity theft. As the ability to collect and store data electronically has grown, so has the crime of identity theft. Requiring entities that collect, maintain, or transfer consumer data to meet basic safeguards will go a long way in preventing these crimes.

The regulations define personal information as an individual's last name, first name or first initial, linked with a Social Security Number, Drivers License Number, or account number. This is very specific data, which should only be collected in certain circumstances. This kind of data should not be collected in large databases by average businesses. Entities that do collect this type of data must be help responsible and accountable to reasonably protect it from a security breach and ending up in the hands of identity thieves.

We understand that many business organizations are critical of the regulations. But these regulations are commonsense measures such as designating an employee to design and implement protections, identifying potential security risks, inventorying data containing personal information so it can be protected, preventing terminated employees from accessing said data, and making sure only appropriate employees have access to consumers' personal information.

Thank you for the opportunity to comment on the regulations. Please feel free to contact me for questions or comments.

Eric Bourassa
Consumer Advocate



January 12, 2009

Governor Deval Patrick
Massachusetts State House
Office of the Governor
Room 360
Boston, MA 02133

Secretary Daniel O'Connell
Executive Office of Housing & Economic Development
One Ashburton Place, Room 2101
Boston, MA 02108

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

RE: Top Priority- Protect Personal Information through Stakeholder Analysis

Dear Governor Patrick, Secretary O'Connell and Undersecretary Crane:

As an employer with 23 employees, I am very concerned, about the mandates currently included in 201 CMR 17.00. As written, these regulations set a perilous course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth. I urge the Patrick's Administration Patrick's Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 with the Department, Attorney General, regulated community and elected officials, to re-issue an entire set of rules by May 1, 2009 with implementation of the rules over a two year period.

As a business owner or employee the protection of personal information for residents of the Commonwealth is a top priority. The delay in the effective date is helpful, as a practical matter, it is unreasonable to believe that my firm has a fair opportunity to reach full compliance. As currently written, 201 CMR 17.00 goes beyond the legislature's intent and mandates specific technologies, creates redundant and confusing rules and does not hold public agencies to the same standards of the private sector. In many instances the regulatory mandates are not technically or economically feasible for public or private agencies regardless of size or available resources. Further, the regulations do not envision the national and global business relationships that the Massachusetts economy depends on.

MAIN OFFICE

258 MAIN STREET
TEL: 508.347.6850

P.O. BOX 1220
800.342.3859

STURBRIDGE, MA 01566
FAX: 508.347.6855

NORTH BROOKFIELD

169 MAIN STREET
TEL: 508.867.6411

NORTH BROOKFIELD, MA 01535-1473
FAX: 508.867.5948

The implications of 201 CMR 17.00 will have a negative impact on “all persons” and all firms that conduct business in Massachusetts. The promulgation and implementation of these specific regulations are in sharp contrast with other states and especially other Massachusetts state agencies that routinely engage in collaborative discussions with the regulated communities. The state of New Jersey recognized the need for a vigorous stakeholder analysis. Currently, the State of New Jersey is currently in a two year process just to promulgate a “pre-proposal” of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey’s new pre-proposal provides for a comment period until February 13, 2009. Regrettably, the Massachusetts regulations do not provide similar time, clarity, recognition of federal regulations nor do they recognize the significant technological, legal, operational challenges or the significant investments and human talent that many persons and small firms must now face.

The following is a partial list of the issues and solutions that the business community has identified:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules to achieve the ultimate goal of compliance. The regulations should be implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Otherwise the contract and written certification requirement becomes a never ending, complex, costly, and circular mandate virtually without end.

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute. A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology.

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated. A better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. The risk assessment approach would be similar to what is required in other federal and state contexts.

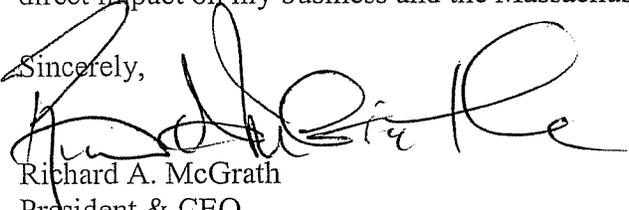
Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations. Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy

Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose

Under these rules "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 to "all persons" or firms, regardless of readily available resources.

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. Thank you for considering the long-term implications of these regulations and their direct impact on my business and the Massachusetts economy.

Sincerely,



Richard A. McGrath

President & CEO

McGrath Insurance Group Inc.

Cc: Senator Michael W. Morrissey, Chairman
Committee on Consumer Protection & Professional Licensure

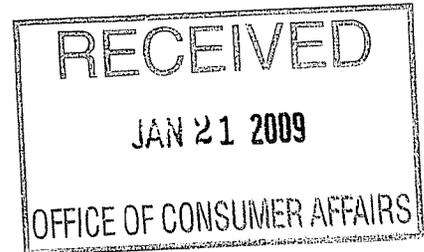
Rep. Michael J. Rodrigues, Chairman
Committee on Consumer Protection & Professional Licensure



MELICK, PORTER & SHEA, LLP
COUNSELLORS AT LAW

Adam M. Guttin
(617) 502-9608
FAX: (617) 502-9708
aguttin@melicklaw.com

January 20, 2009



RICHARD J. SHEA
ROBERT P. POWERS
JOHN F. ROONEY, III *(CT, DC & NH)
WILLIAM D. CHAPMAN
MICHAEL J. MAZURCZAK *(NY & WI)
ROBERT T. TREAT
WILLIAM L. KEVILLE, JR.
ANDRE A. SANSOUCY
ROBERT R. HAMEL, JR.
JENNIFER B. HARDY
DONNA M. MARCIN
VINCENT P. DUNN *(NH)
JOHN J. REARDON
MAUREEN E. LANE *(NH)
ADAM M. GUTTIN *(RI)
T. DOS URBANSKI *(RI)
MEGAN E. KURES
JESSICA M. FARRELLY *(FL)
MATTHEW GRYGORCEWICZ
DEBRA I. LERNER *(DC & TX)
ALEXANDRA POWER
ERIN J.M. ALARCON *(NH)
J. PAUL VANCE, JR. (CT ONLY)
NICOLE L. COOK *(NH)
RAYMOND H. TOMLINSON, JR.
JOHN A. CALETRI *(RI)
CINDY PEAN
SHANNON M. MCQUEENEY *(NY)
PATRICK D. BANFIELD *(RI & CT)
SEEMA A. LYNCH
JULIE T. FISHER
W. PRESCOTT GOLDING, JR. *(ME)
KATHRYN M. AUGER
ROBERT S. LUDLUM *(NY & CT)
DOUGLAS F. HARTMAN
LISA WICHTER *(NY)
MICHAEL G. WINTERS
JONATHAN M. WHITE
LEONARD D. ZAMANSKY *(NH)

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

Re: Comments in response to Regulations on Standards for the Protection of
Personal Information of Residents of the Commonwealth

Dear Madam and Sirs:

The following are comments to the regulations. We appreciate your
consideration of our comments.

Section 17.03 (f)

Section 17.03 (f)(ii) requires companies to take reasonable steps to verify that
third-party service providers with access to personal information have the
capacity to protect such information and *contractually require* service providers
to maintain such safeguards. The regulation further requires that prior to
permitting third-party service providers access to personal information, the person
permitting such access shall obtain from the third-party service provider a *written
certification* that such service provider has a written, comprehensive information
security program that is in compliance with the regulations. This regulation is
unnecessary. To the extent a service provider has access to personal information
on a Massachusetts resident, they would already be covered by the regulations.
Furthermore, it would be unduly burdensome and costly for companies to have to
attempt to renegotiate existing contracts and obtain a service providers agreement
and written certification on a contract that has already been executed.
Consequently, we would request that you delete Section 17.03(f).

Section 17.03 (g) and (i) and 17.04 (4)

The regulations would call for major changes to many companies' computer
networks and systems. For example, these sections would require auditing
employee access, access to the smallest number of persons who are reasonably
required to know such information in order to accomplish such purpose, and
recording the audit trails for users, events, dates, times and success or failure of
login. Such changes will take significant time for many companies to modify

OF COUNSEL
THOMAS W. PORTER, JR.

*ALSO ADMITTED

28 STATE STREET
BOSTON, MA 02109
(617) 523-6200
FAX (617) 523-8130

4 COURT STREET, SUITE 222,
PLYMOUTH, MA 02360
(508) 746-2282
FAX: (877) MPS-1322

49 WEYBOSSET STREET
PROVIDENCE, RI 02903
(401) 941-0909
FAX (401) 941-6269

65 BANK STREET
WATERBURY, CT 06702
(203) 596-0500
FAX (203) 596-0040

MELICKLAW.COM

Melick, Porter & Shea, LLP
January 20, 2009
Page 2

existing networks and systems to accomplish these regulations. In light of the current economy, many companies are cutting back both on expenses and personnel and consequently have limited resources to make the significant changes required by these regulations. We would propose that the regulations grant a minimum of three years to allow companies adequate time to make such significant system wide changes. Consequently, we would recommend adding the following statement to Sections 17.03 and 17.04: "Any system changes necessitated by these regulations must be implemented within three years of the effective date of the regulations."

If you have any questions about our comments or would like to discuss them further, please do not hesitate to give me a call. Again, we thank you for your time and for your consideration.

Very truly yours,


Adam M. Guttin

AMG/ks

Melick, Porter & Shea, LLP
January 20, 2009
Page 3

bcc: Cari Curtis (by fax 281-348-3908)



MHSACM, Inc.

251 West Central Street, Suite 21, Natick, MA 01760 (508) 647-8385 / Fax (508) 647-8311 www.mhsacm.org

Vicker V. DiGravio III, *President / CEO*

Deborah Ekstrom, *Chair*

January 16, 2009

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

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

Dear Mr. Murray:

On behalf of the membership of Mental Health and Substance Abuse Corporations of Massachusetts, Inc. (MHSACM), thank you for the opportunity to submit testimony relative to proposed amendments to *201 CMR 17.00, Standards for the Protection of Personal Information of Residents of the Commonwealth*. MHSACM is a statewide organization representing 91 community mental health and substance abuse providers across the state. MHSACM members serve approximately 117,000 clients daily and employ approximately 22,000 individuals.

MHSACM appreciates that the proposed amendments delay the compliance dates for obtaining a certification from third party service providers and for encrypting portable devices other than laptops until January 1, 2010 and the compliance date for all other provisions until May 1, 2009. However, we remain concerned that, even with the delayed implementation dates, these regulations will result in significant costs and administrative burdens for mental health and substance abuse provider organizations across the Commonwealth. We urge you to reconsider some of these requirements and consider the possibility of allowing organizations more time to comply with the regulations.

CONTRACT PROVISIONS AND WRITTEN CERTIFICATIONS

Many mental health and substance abuse provider organizations contract with third-party entities. While providers are obviously concerned with protecting any personal data sent to these entities, the requirement that organizations obtain both contract provisions and written certifications is duplicative. We encourage the regulations to require only contract provisions. Requiring providers to obtain written certification from third-party entities will create a financial and bureaucratic burden and divert resources from service provision to paperwork.

COMPUTER SYSTEM SECURITY REQUIREMENTS

MHSACM understands the need to establish and maintain a computer security system in order to protect personal data. At the same time, many behavioral health providers are very small

organizations (some with as few as four employees) and simply do not have the IT capability and/or resources to comply with these requirements. We urge you to further extend the compliance deadline in order to give organizations more time to meet the requirements.

MHSACM providers are especially concerned about the mandatory encryption provision. The provision is extremely prescriptive; furthermore, behavioral health providers operate on limited resources and mandating encryption of all laptops and portable devices will be especially burdensome. Provider organizations are already operating on razor-thin margins and cannot simply raise prices to pass along added costs to purchases. MHSACM urges you to reconsider this blanket requirement and instead implement a standard for organizations to follow rather than a prescriptive encryption mandate.

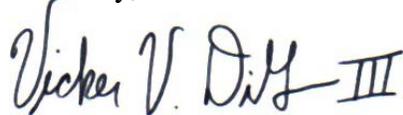
CLARIFICATION

201 CMR 17.03 states that compliance the comprehensive information security program will take into account “the size, scope and type of business”. While we appreciate that the regulations take these factors into consideration, this provision, as it is currently written, is unclear. In order to foster compliance, we urge you to clarify this section.

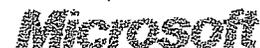
MHSACM provider organizations recognize the importance of protecting the personal information of both their employees and their clients. At the same time, legitimate concern exists surrounding the potentially burdensome implications of implementation. MHSACM members are the primary providers of publicly-funded mental health and substance abuse services for children, adolescents, and adults across Massachusetts. The recent 9C cuts coupled with the extremely dismal FY 2010 budget outlook have placed an already financially unstable system at even greater risk. It is simply not feasible to ask providers to take on additional financial and administrative burdens at this time. As such, we respectfully request that you will consider these concerns as you evaluate the proposed amendment to these regulations. At the very least, we encourage you to provide organizations with additional time to comply with these extensive requirements.

Thank you for your time and consideration.

Sincerely,

A handwritten signature in black ink that reads "Vicker V. DiGravio III". The signature is written in a cursive style with a long horizontal line extending from the end.

Vicker V. DiGravio III
President & CEO



January 15, 2009

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

Re: **201 CMR 17.00**

Dear Undersecretary Crane,

I would like to thank you and the Office of Consumer Affairs and Business Regulation for your decision to extend some of the compliance dates for 201 CMR 17.00. We strongly support your statement that "[t]hese sensible measures are already widely used by many Massachusetts companies, but we recognize that some businesses, currently facing economic uncertainties, will benefit from having additional time to comply."

In the last few weeks, we have continued to examine the potential impact that these regulations would have on Microsoft's business. We have confirmed our prior conclusions that there are fundamental deployment challenges with both the encryption and other provisions of the regulations. Even with the extension, full compliance with these regulations will be virtually impossible for several years, until significant costs have been incurred to replace existing data storage and transmission hardware and software with more sophisticated and interoperable systems. This will be very difficult for Microsoft as a technology company, and it will be virtually impossible for entities with fewer resources and less technical sophistication. In support of this, I respectfully re-submit my written testimony, which was originally submitted to the Joint Committee on Consumer Protection & Professional Licensure in November 2008.

Microsoft fully supports the goals behind the regulations and Massachusetts statute, and we recognize the need to create safeguards to protect the personal information of Commonwealth residents. We have a long-standing commitment to data security in our own products. Microsoft's Office Outlook[®] offers email encryption through technologies like S/MIME and PKI and has done so for many years. Certain Windows operating systems feature encryption technologies such as Windows Vista[™] BitLocker[™] Drive Encryption[™] -- but this technology is not enabled by default in Windows Vista[™] nor will it be included in all versions of the forthcoming Windows 7 (as it will only be available in certain high- end versions of the product). These Microsoft encryption technologies are not available at all in older versions of Windows such as the still widely-used Windows XP and Windows 2000.



While these and other similar hard-drive encryption technologies are available, they cannot be deployed quickly in distributed computing environments and require labor-intensive, manual installations on one computer at a time -- assuming the hardware meets certain performance specifications. In addition, it can take years for this data storage or data transmission technology to reach widespread adoption. This is a crucial point - for communications to be effectively encrypted, the sender and the recipient must be using the same or at least interoperable products. The necessary software upgrades to comply with the regulations will be expensive and time consuming to implement; the hardware upgrades will be even more expensive.

Here are some additional concerns we have with the language of 201 CMR 17.00 as currently written:

- The regulation is significantly more prescriptive and broader in applicability than the underlying language of the Massachusetts statute (M.G.L. c. 93H). In addition, the requirements of the regulation itself are inconsistent, stating first that "protection of personal information shall be evaluated taking into account (i) the size, scope and type of business," and then mandating encryption and other prescriptive technical controls for all "persons" operating in Massachusetts without regard for the size or type of organization.
- Some of the technical controls mandated by the regulation are not feasible in today's computing environment with available technologies and/or resources. A vivid example of this is found in the inventory requirement of §17.03(h) which requires organizations to identify paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, and to determine which records contain personal information (except when a comprehensive information security program provides for the handling of all records as if they all contained personal information). Microsoft has deployed data scanning technology on a pilot basis, and has discovered that there are significant hardware and network constraints that make it impossible to deploy the technology in a manner that is currently required by the regulations. Current scanning technologies using a single dedicated scanning computer can scan about 190GBytes per day over a corporate network. Six dedicated high end computers can scan about 1 TeraByte per day. Assuming that the average enterprise has about 5 Petabytes of data it would take over a year to do an initial scan (5000 days). To perform this scan in 180 days it would take over 150 dedicated high end computers working full time, and this does not account for the additional network bandwidth that would be required. This is an optimistic calculation since no company currently has the network or CPU resources to do electronic document scanning of this scale across all systems and storage technologies. Likewise, the alternative i.e. handling all records as if they all contained personal information, would be a multi-year undertaking, incurring significant costs to most mid-size and large businesses.

From: Chisholm, Paul [paul.chisholm@mindshift.com]
Sent: Wednesday, January 21, 2009 9:34 AM
To: Murray, David (SCA)
Subject: FW: Data Privacy Regulations 201 CMR 17

Dear Mr. Murray,

As the CEO of an IT services company headquartered in Massachusetts with 390 employees in four key states (Massachusetts, New York, Pennsylvania and Virginia), I am writing to support the recommendations and suggested modifications made by the Greater Boston Chamber of Commerce in regards to the Data Privacy Regulations. Although there is a need to insure stricter standards to protect individuals and businesses, the scope and magnitude of the changes would put a burden on all businesses trying to comply with the proposed law. I believe that several requirements within the proposed regulation merit further discussion and consideration prior to their implementation.

At a time when the economy is affecting everyone, there is no need to increase the burden to all businesses, large or small. I support an approach that furthers our commonly shared goals of protecting personal information while also growing the economy. Therefore, I strongly suggest that the Office of Consumer Affairs and Business Regulation adopt the Chamber's suggestions and again extend the time for all businesses to comply with the new regulation.

Thank you for your kind consideration.

Paul W. Chisholm
Chairman & CEO
mindSHIFT Technologies
307 Waverley Oaks Road, Suite 201
Waltham, MA 02452
Tel: 617-243-2748
Cell 781-526-2005
Fax 617-243-2799
www.mindshift.com

Boston-New York-Philadelphia-Washington, DC
We make IT work for your business.®

 Please consider the environment before printing this e-mail



MASSACHUSETTS

Testimony of

Bill Vernon, State Director, National Federation of Independent Business
Relative to 201 CMR 17.00 et seq.
Before the Office of Consumer Affairs and Business Regulation
January 16, 2009

Undersecretary Daniel C. Crane and General Counsel David A. Murray:

My name is Bill Vernon. I am the Massachusetts Director of the National Federation of Independent Business (NFIB). A non-profit, non-partisan organization, NFIB is the nation's and our state's largest small business advocacy group. In Massachusetts, NFIB represents thousands of small and independent business owners involved in all types of industry, including manufacturing, retail, wholesale, service, and agriculture. The average NFIB member has five employees and annual gross revenues of about \$450,000. In short, NFIB represents the small Main Street business owners from across our state. On behalf of those small and independent business employers in the Commonwealth, I urge you to review carefully the financial impact of these regulations on small businesses in the Commonwealth, particularly in light of the current economic climate, and to ask yourself whether there is a more reasonable way to accomplish our mutual goal of protecting individual privacy.

NFIB members are concerned about the compromise of private personal information. NFIB members are Massachusetts consumers who want their personal information protected. That is why NFIB did not vigorously oppose enactment of the enabling legislation, M.G.L. c. 93H. But NFIB is concerned that certain provisions of the proposed regulations promulgated pursuant to that legislation may unnecessarily threaten to impose a substantial negative economic impact on small businesses.

The small business impact statement issued with the proposed regulations -- one of the best I have ever seen in Massachusetts -- admits to expenses for each small business that could be several thousand dollars up front with annual maintenance fees of hundreds of dollars depending on the current state of the particular business's computer system. Although cost estimates are preliminary, given the number of small businesses in the Commonwealth, it is likely that total expenses for the small business community in Massachusetts will exceed \$1 billion in the first two years of implementation. The high cost of doing business in Massachusetts is well documented. Adding this type of cost at this time is not a wise public policy choice.

Allow me to address specific concerns related to small businesses. First, is the agency's insistence to date on a comparatively short time frame for implementation. From a small business owner's point of view, it is extremely important to protect an individual's personal information from unwarranted disclosure as soon as possible, but at this time I can safely report that the lack of knowledge among small business owners about these regulations is a significant barrier to compliance. Additional time will increase compliance by affording regulators an opportunity to get these regulations right, to incorporate changes that have been suggested by knowledgeable and interested parties, to eliminate unnecessary and duplicative requirements, and to inform affected individuals and businesses of prospective.

Secondly, while the statute specifically requires levels of responsibility based on the size of the business enterprise, the regulations provide no differentiation – just an assertion (promise) that the state government will differentiate among the businesses in enforcement and punishment based on size. The 'carve out' for small businesses should be substantive and be specifically stated in the regulations.

Third, the statute clearly states that no private right of action under M.G.L. c. 93A should arise from these regulations and yet such a provision is not included. It is a simple matter to include such a prohibition in the regulations. Without it, the regulations potentially create a new cause of action in civil liability law for trial lawyers to sue small business owners. This is a major issue for small business owners who know that a law suit, whether meritorious or frivolous, is a constant threat to the continuation of their business. The regulations must restrict actions under M.G.L. c. 93A to protect small business owners acting in good faith from law suits based on these regulations. The expansion of legal causes of action would adversely impact the state's business climate at a time when most believe we should be doing all we can to encourage businesses to grow and preserve and create jobs.

Finally, I am concerned that the proposed regulations pose a unique problem and probably almost impossible task for small business owners seeking to procure certifications of compliance from out-of-state third party vendors. The reluctance of third party vendors to spend any resources to comply, the concern of third party vendors of possible legal action for any compromise of personal private information, and the relatively small business relationship between out-of-state vendors and domestic small businesses will probably force our small businesses to discontinue relationships and to seek new suppliers and customers.

NFIB supports the delineation of issues and suggested solutions outlined in the coalition letter dated January 9, 2009, i.e. encryption should not be specifically mandated and required only at the time of computer upgrade; third party vendor certification requirement should be delayed until January 1, 2011, and then only upon renewal of contracts; and a level playing field should be created to hold public agencies to the same standards as private firms.

There is no debate that these regulations will be costly to small business owners. NFIB requests that you act to limit these costs however and wherever possible, to ensure compliance and accomplishment of our goals without further damaging Massachusetts' business climate.

Again, NFIB is ready to work with you to accomplish our mutual goal of safeguarding personal privacy in a cost effective and reasonable way. Thank you.

From: bounce@bounce.votervoice.net on behalf of David Peterson [david.peterson@netscout.com]
Sent: Tuesday, January 13, 2009 12:35 PM
To: General Counsel David Murray
Subject: Change Mass. Data Regulations

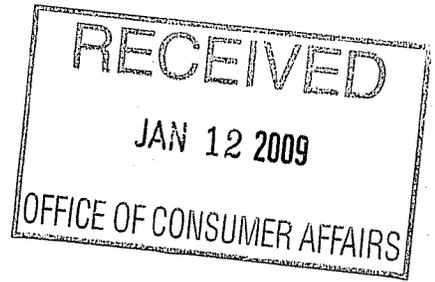
General Counsel Murray:

As an employer in the town of Westford, MA with 800 worldwide employees, I am very concerned about the mandates currently included in 201 CMR 17.00. As written, these regulations set a difficult course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth.

Our company, similar to most organizations, do not have the resources or the technical infrastructure to comply with the regulations by May 1, 2009. There are no tools, forms or guidelines, or templates to help companies such as Netscout, who are all-ready resources constrained, to help comply with the regulations. Lastly, these regulations will add additional expense to the business at a time when budgets are getting slashed.

Sincerely,

David Peterson
7 Quail Dr
Medway, MA 02053



January 8, 2008

Governor Deval Patrick
Massachusetts State House
Office of the Governor
Room 360
Boston, MA 02133

Secretary Daniel O'Connell
Executive Office of Housing & Economic Development
One Ashburton Place, Room 2101
Boston, MA 02108

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

Top Priority: Protect Personal Information through Stakeholder Analysis

Dear Governor Patrick, Secretary O'Connell and Undersecretary Crane:

As a small business employer of 5 employees, I am very concerned, about the mandates currently included in 201 CMR 17.00. As written, these regulations set a perilous course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth. I urge the Patrick's Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 with the Department, Attorney General, regulated community and elected officials, to re-issue an entire set of rules by May 1, 2009 with implementation of the rules over a two year period.

As a business owner or employee the protection of personal information for residents of the Commonwealth is a top priority. The delay in the effective date is helpful, as a practical matter, it is unreasonable to believe that my firm has a fair opportunity to reach full compliance. As currently written, 201 CMR 17.00 goes beyond the legislature's intent and mandates specific technologies, creates redundant and confusing rules and does not hold public agencies to the same standards of the private sector. In many instances the regulatory mandates are not technically or economically feasible for public or private agencies regardless of size or available resources. Further, the regulations do not envision the national and global business relationships that the Massachusetts economy depends on.

The implications of 201 CMR 17.00 will have a negative impact on "all persons" and all firms that conduct business in Massachusetts. The promulgation and implementation of these specific regulations are in sharp contrast with other states and especially other Massachusetts state agencies that routinely

engage in collaborative discussions with the regulated communities. The state of New Jersey recognized the need for a vigorous stakeholder analysis. Currently, the State of New Jersey is currently in a two year process just to promulgate a "pre-proposal" of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey's new pre-proposal provides for a comment period until February 13, 2009. Regrettably, the Massachusetts regulations do not provide similar time, clarity, recognition of federal regulations nor do they recognize the significant technological, legal, operational challenges or the significant investments and human talent that many persons and small firms must now face.

The following is a partial list of the issues and solutions that the business community has identified:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules to achieve the ultimate goal of compliance. The regulations should be implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community.

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Otherwise the contract and written certification requirement becomes a never ending, complex, costly, and circular mandate virtually without end.

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute. A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology.

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated. A better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. The risk assessment approach would be similar to what is required in other federal and state contexts.

Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations. Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy.

Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose

Under these rules "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 to "all persons" or firms, regardless of readily available resources.

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. Thank you for considering the long-term implications of these regulations and their direct impact on my business and the Massachusetts economy.

Sincerely,



Carol F. Wilson, CIC
President

cc: Cory Atkins, State Representative
Susan Fargo, State Senator

CONFIDENTIAL



NORTH CENTRAL
MASSACHUSETTS
CHAMBER OF COMMERCE

January 21, 2009

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

Re: Protect Personal Information through Stakeholder Analysis

Dear Undersecretary Crane:

Representing 1500 businesses, with over 49,000 employees in the cities and towns in the north central region of Massachusetts, I write in regards to the department's proposed data breach regulations. The North Central Massachusetts Chamber of Commerce and our member companies believe the protection of personal information is a top priority. However, I have to express our deep concern over many of the requirements of 201 CMR 17.00.

Late last year, the Chamber's Human Resources Council held a forum to brief human resource professionals on the requirements contained in the regulations. All in the room expressed frustration and apprehension over their company's ability to adequately satisfy the requirements of the regulations. Many left with more questions than answers. The department's delay in the effective date to May, 2009 is helpful, but it is still unreasonable to believe that businesses will be able to reach full compliance given the structure and mandates of the rules themselves.

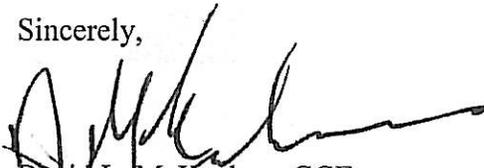
A possible solution to the many issues expressed by the business community is to delay the full implementation for two years. If businesses are not clear on what they are required to do, compliance will be more difficult to achieve. Massachusetts residents will be better protected by the establishment of clear guidelines. By allowing for implementation over a two year period, Massachusetts businesses will be better prepared to protect personal data.

The additional mandates on businesses come at a time when many are already facing economic difficulties. In addition to general economic concerns, the North Central economy continues to feel the impacts of the ice storm of December, 2008 when many residents and businesses were without power for multiple days. Commerce was affected in numerous ways from the shut down of manufacturers because their labor force could

not travel on impassible roads to dry cleaners without power for days. As an example, one manufacturer was without power for 12 days -- without the ability to meet their orders, this company lost numerous sales and revenue. Under these regulations, this small manufacturer will now need to hire an information technology professional and possibly purchase a new computer system to ensure compliance.

I respectfully urge the administration to reconsider the impact of these regulations. We all agree the protection of the personal information of Massachusetts residents is necessary but the current regulations and implementation schedule are not achievable. I respectfully ask for the regulations to be rewritten and implemented over a two year period to allow for proper preparation and education by the business community.

Sincerely,

A handwritten signature in black ink, appearing to read "D. McKeehan", with a long horizontal flourish extending to the right.

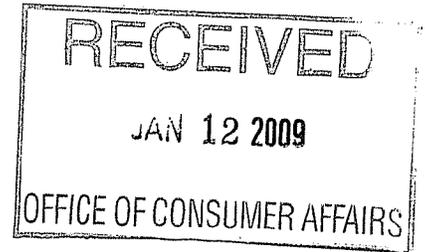
David L. McKeehan, CCE
President

O'BRIEN'S

Centerville Insurance Agency, Inc.

January 8, 2009

Daniel Crane, Undersecretary
Office of Consumer Affairs & Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116



Dear Mr. Crane,

RE: amendments to 201 CMR 17.00

As the owner of a small family-owned insurance agency, I am extremely concerned about meeting the May 1, 2009 deadline for compliance with the data privacy law. There are practical, technical and economic challenges in implementing the regulations properly in order to protect personal data in the most efficient and cost effective way that will require additional time beyond that deadline. A more appropriate deadline would be January 1, 2010.

We would like to urge your administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations with the OCABR, the Attorney General, regulated community and elected officials. These are the strictest data privacy laws in the nation and there is a critical need to address the underlying deficiencies in these regulations before they are implemented.

Thank you for your attention to this important matter.

Sincerely,

A handwritten signature in black ink that reads "Stephen B. O'Brien Jr." in a cursive style.

Stephen O'Brien, President

cc: Senator Michael W. Morrissey, Chairman
Representative Michael J. Rodrigues, Chairman
Committee on Consumer Protection & Professional Licensure



From: Paul Bowen [pbowen@artsecret.com]
Sent: Thursday, January 15, 2009 10:41 PM
To: Murray, David (SCA)
Subject: Massachusetts Data Breach Regulations

Good evening,

I am writing in support of these. I just attended a presentation by the Associated Industries of Massachusetts given by Brad MacDougall. I was horrified by his warped presentation which in my expert technical opinion, was seriously flawed. It was very apparent that he and this group are engaged in a campaign meant to induce fear, uncertainty and doubt.

Although no one will ever agree on a single perfect law, I feel you are off to a good start and through progressive elaboration and changes after implementation; the consumers of Massachusetts will be well served by its implementation. I urge you to proceed with implementation as soon as is practical. If it were not for steps like these, the average consumer would still be subject to tainted food and medicine. The simple fact of the matter is that a business which can not afford to properly maintain personally identifiable information, PII, should not be in business. The consumers of Massachusetts have long been baring the burden of rampant negligence on the part of business in the area of PII protection. If it were not for the groundbreaking California law, consumers would still be in the dark on hundreds of millions of exposures. It is businesses have been responsible for these losses which have led to untold losses by individual consumers.

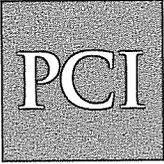
Business should be regulated to at least put in a minimum effort in the protection of PII. I do not envision the Commonwealth of Massachusetts imprisoning someone who does their mothers taxes and losing the information as Mr. MacDougall hypothesized in his presentation tonight.

The United States is currently going through a very difficult period as a direct result of business failing to self regulate. Again I urge you to proceed as soon as is possible and would actually request that you increase consumer protection to allow consumers to put no cost credit freezes on their credit records as has been requested by consumer advocates. The negligence of businesses have cost consumers and enriched the credit bureaus which charge for credit monitoring when a far simpler solution is the freezing of credit.

Thank you,

Paul

Paul Bowen
MS IT Information Security, CISSP, MCSE, PMP



**Property Casualty Insurers
Association of America**

Shaping the Future of American Insurance

40 Court Street, Suite 700, Boston, MA 02108

January 16, 2009

Mr. Daniel C. Crane
Undersecretary
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116

Dear Mr. Crane:

Attached please find the statement of PCI for the January 16, 2009 hearing by the Office of Consumer Affairs and Business Regulation relating to the emergency amendments to Regulation 210 CMR 17.00.

Given the fundamental flaws with the regulation, we are hopeful that it can be suspended indefinitely so that we can work with you and others in the Patrick Administration to address the legitimate concerns of the business community and others affected about this regulation.

Thank you for your consideration of this matter.

Very truly yours,

A handwritten signature in black ink that reads "Francis C. O'Brien". The signature is written in a cursive style with a long horizontal flourish at the end.

Francis C. O'Brien
Vice President, Regional Manager and Counsel

FCO:am



**Property Casualty Insurers
Association of America**

Shaping the Future of American Insurance

2600 South River Road, Des Plaines, IL 60018-3286

**STATEMENT FOR THE JANUARY 16, 2009 HEARING BY THE OFFICE OF
CONSUMER AFFAIRS AND BUSINESS REGULATION REGARDING
EMERGENCY AMENDMENTS TO REGULATION 210 CMR 17.00**

The Property Casualty Insurers Association of America ("PCI") submits this statement to the Office of Consumer Affairs and Business Regulation ("OCABR") in connection with the hearing being held on January 16, 2009 concerning the emergency amendments to regulation 210 CMR 17.00 (Standards for the Protection of Personal Information of Residents of the Commonwealth) promulgated by OCABR on November 14, 2008. The amendments extend the compliance date to January 1, 2010 for obtaining the certifications from vendors required by the regulation and for encrypting portable devices other than laptop computers, and they extend the compliance date to May 1, 2009 for the other provisions of the regulation.

PCI is a national property/casualty insurance company trade association, with more than 1,000 members whose annual premiums total almost \$200 billion. PCI members account for 40.5% of total property/casualty premiums in the United States.

First, PCI wants to applaud OCABR for the compliance delays adopted by the emergency amendments, limited though they are. Unfortunately, those delays are not long enough and do not do nearly enough to resolve the fundamental, persistent problems with the regulation. PCI belongs to the large coalition of businesses, business trade associations in Massachusetts and around the country, and others affected by the regulation, and we share the concerns of that coalition with many aspects of the regulation that have been previously expressed to OCABR, others in the Patrick Administration and to the Legislature's Joint Committee on Consumer Protection and Professional Licensure.

While the principal purpose of the hearing may be to take comments on the amendments, we believe it is essential that OCABR accept and pay close attention to comments regarding the remaining, broader problems with the regulation, which go beyond the revised compliance dates. Among the principal problems with the regulation are the following:

Non-Compliance with Enabling Statute. There are at least three areas where the regulation does not take into account or does not comply with significant provisions of the enabling statute:

- The enabling statute requires that the regulations "shall be consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated." G.L. c. 93H, § 2(a). 201 CMR 17.00 et seq. goes far beyond any existing federal safeguards.

▪ The enabling statute includes the following requirement for any regulation that is promulgated: "The regulations shall take into account the person's size, scope and type of business, the amount of resources available to such person, the amount of stored data, and the need for security and confidentiality of both consumer and employee information." G.L. c. 93H, § 2(a). The regulation promulgated by OCABR only provides for such differentiation in an after-the-fact evaluation of whether the required comprehensive information security program for a subject person is in compliance with the regulation. This is clearly not what the Legislature had in mind in imposing this requirement and limitation. In reality, it leaves businesses with no idea what the standards are and, in effect, makes them subjective. As evidenced by the letter dated October 16, 2008 to you from the Massachusetts Association of Insurance Agents, which is made up of many small or smaller businesses, the type of differentiation in obligations required by the enabling statute is essential if the regulatory scheme is to be fair and workable.

▪ G.L. c. 93H, § 5 provides in relevant part as follows: "... [A] person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; provided further that the person also notifies the attorney general and the director of the office of consumer affairs and business regulation of the breach as soon as practicable and without unreasonable delay following the breach." The OCABR regulation contains no recognition of this statutory exemption from the Massachusetts requirements. The regulation should be revised to reflect this provision.

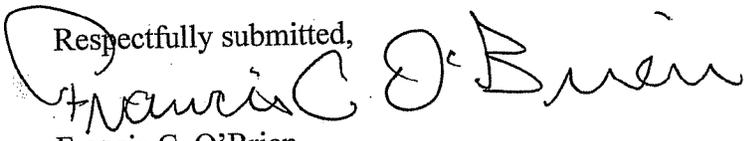
• **Overly Rigid Standard of Encryption.** The enabling statute defines "encrypted" as "transformation of data through the use of a 128-bit or higher algorithmic process into a form *in which there is a low probability of assigning meaning without use of a confidential process or key.* ..." G.L. c. 93H, § 1(a). (Emphasis supplied.) The OCABR regulation defines the term "encrypted" as "the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key. ..." Thus, by converting the words "low probability of assigning meaning" in the statute into "meaning [that] cannot be assigned," the regulation has made the standard for encryption much more rigid than the one contained in the enabling statute, and we think unreasonably so. PCI recognizes that the Legislature has explicitly given the OCABR the authority in the definition of "encrypted" in the statute to revise that definition; however, we think the definition in the regulation should be further revised. The AeA has submitted in its letter of October 21st to Secretary O'Connell a definition that preserves the more flexible language of the statute and has the added advantage of having been used in more than 30 states and having been adopted in model legislation by the American Legislative Exchange Council.

• **Vendor Certification.** While the emergency amendments delay the compliance date for obtaining the required certifications of compliance with the regulation from vendors until after January 1, 2010, that change is not sufficient. We

think that the vendor certification method is still not reasonable or appropriate. The certification requirement improperly delegates enforcement of the regulation to the regulated entity, and increases the likelihood that it will fail to comply due to non-compliance by its vendors. At most, there should not be a fixed, arbitrary deadline for the requirement; instead, any requirement should be allowed to be incorporated in vendor agreements as they are normally revised.

Given the fundamental flaws with the regulation, we are hopeful that it can be suspended indefinitely so that we can work with you and others in the Patrick Administration to address the legitimate concerns of the business community and others affected about this regulation.

Respectfully submitted,


Francis C. O'Brien

Vice President, Regional Manager
and Counsel

PROVIDERS'
COUNCIL
for caring communities

To: Daniel Crane, Undersecretary
David Murray, General Counsel
Office of Consumer Affairs and Business Regulation

From: Michael Weekes, President/CEO
The Providers' Council

Re: Testimony on 201 CMR 17.00 – ***Standards for the Protection of Personal Information of Residents of the Commonwealth.***

Date: January 16, 2009

Undersecretary Crane, thank you for this opportunity to address you. The Providers' Council is a statewide association of home- and community-based caregivers contracting with state purchasing agencies to deliver a wide array of rehabilitation, education, health and social services. The Council is the state's largest association of human service providers, and it represents an industry that receives more than \$2.7 billion from the state – approximately 10 percent of the state budget – through the Executive Office of Health and Human Services (EOHHS).

Our organization is submitting this testimony regarding 201 CMR 17.00 – *Standards for the Protection of Personal Information of Residents of the Commonwealth*. First, we should state that protecting the privacy and the confidentiality of the people served by our sector has always been of great importance to us, and, to that end, we endeavor to comply with all reasonable procedures and guidance.

We are a sector that is mandated by the state to provide essential human services to our most vulnerable residents. In order to fulfill that mandate, it is necessary for us to maintain non-public information to assure effective service delivery. Typically, this information does not include credit card numbers or other specific financial data. While it is not clear if our sector was targeted for this legislation, our interpretation is that the encryption requirement is inclusive of our sector. We assert that compliance with this will be onerous and costly – not only to our sector, but also to our primary funding source, the Commonwealth of Massachusetts.

Implementation of these regulations will only deepen the well-documented financial ills of human service organizations that provide essential core services to the vulnerable residents of the Commonwealth.

Our Request

We appreciate the fact that the deadline for complying with these regulations has been extended to May 1, 2009. Having an extra four months, however, will not relieve us of the burden of compliance. Accordingly, we ask that our state contracted human service sector be exempt from compliance with 201 CMR 17.00. Our reasons follow:

1. Sector as extension of government

The people served by our sector are referred to us by the Commonwealth mostly through “closed referral contracts.” We are a virtual extension of the state as we work to fulfill explicit legislative mandates and comply with all state requirements and related federal regulations with which the state also complies. This is well defined in the contracts of our sector with the Commonwealth. Typically our sector engages in no commercial activity and its members do not accept commercial purchasing methods, such as credit cards, for any of their financial transactions. Any exchange of information is with state government or its approved entities.

Accordingly, we do not believe these regulations were written to cover this sector in its relationship to state government and believe it should be exempt.

2. Cost prohibitive for sector

Human service providers have been level funded since 1988. Not one additional penny has been appropriated for operating costs since then, and government is the primary source of operating funds. All expenditures are carefully prescribed in maximum obligation contracts to meet the codes and licensing standards of state purchasing agencies. As a result, the budgets of our members are inelastic after years of increased expenses for personnel, fuel, health insurance, occupancy, transportation and similar expenses.

In a time of budget cuts and great fiscal stress, the requirements of these proposed regulations would be crushing to hundreds of human service providers. The funds do not exist to hire the people these new standards require. Further, the IT expertise does not exist within many of our providers to begin to evaluate how to implement them. The funds are not available to procure such assistance from outside vendors. Our basic source of funding is from the state, and it is clearly struggling to provide essential services. Even in positive economic circumstances, the state has no mechanism to reimburse providers for any extraordinary expenses or unfunded mandates.

Again, we thank you for this opportunity. We ask you to give our request your full and positive consideration.



RETAILERS ASSOCIATION
of MASSACHUSETTS

The Voice of Retailing

Testimony of the Retailers Association of Massachusetts
Jon B. Hurst, President
Before the Office of Consumer Affairs and Business Regulation
January 16, 2009
RE: 201 CMR 17.00

Officers

Chairman

Jerome F. Murphy
M. Steiner & Sons
Company, Inc.

Vice Chairman

Larry E. Mulrey
Foodmaster Supermarkets

Secretary

Thomas R. Zapf
Macy's

Treasurer

Howard M. Honigbaum
Ann Soma Co., Inc.

Executive Staff

President

Jon B. Hurst

Vice President

William C. Rennie

General Counsel

Erin M. Trabucco

Membership Director

Andrea K. Shea

Membership Services

Director

Sarah Byrne

On behalf of the Retailers Association of Massachusetts, a statewide trade association comprised of over 3,000 retail companies of all types and sizes, I would like thank you for the opportunity to comment on 201 CMR 17.00. While we are grateful for the delay in implementation, we remain deeply concerned that most businesses will be unable to comply by May 1, 2009. Potential inconsistencies and educational needs for complying with the new FTC Red Flag rules further complicates the situation for Massachusetts employers and organizations. Given the cost and resources needed to comply with this first in the nation regulation, along with the struggles that all businesses are facing during this very difficult economic time, we respectfully request an additional extension of twelve to twenty-four months for the effective date of this regulation, as well as an interested party dialogue, and reconsideration of several provisions contained in this regulation.

RAM continues to believe that this regulation is unnecessary and costly. It is important to remember that consumers continue to be protected financially by employers from the criminal acts of ID theft, and the statute gives consumers and businesses alike the protective tools to fight the crime. Yet, state standards on how the data is protected will create a heavy financial burden-\$300 million in initial costs for small businesses alone under the Administration's impact statement - and opens the door for 50 different standards, when national standards only make common sense in the Internet age. Finally, we have very real concerns over probable 93A actions which may result against local employers for virtually any state reported data breach. The last thing Massachusetts employers, non-profits, and their employees need in this economy is new state regulation that may indeed cost the economy more than the actual crime it is meant to curb.

Consumers and employers alike have taken a beating over the last year, from declining home values, rising energy and food prices, to the recent crashing of 401(k)'s. With consumer confidence down, retailers have been hit particularly hard. To allocate precious money and resources to attempt compliance with this regulation will significantly impact their ability to best serve their customers and recover from the losses they have seen over the past few months. After speaking with several members, we have identified the six components that should be addressed in the regulations.

Duplication and Conflicts With Similar Federal Regulations

In recent months, the Retailers Association of Massachusetts, our 49 counterparts across the country and national industry associations have been working to fully understand and educate our members to the upcoming “Red Flag Rules” of the Federal Trade Commission. These rules will affect thousands of Massachusetts employers that take payments for goods and services on a delayed basis. The intent of these federal rules and this state regulation are exactly the same. We believe it makes common sense and is good public policy to have consistent national standards pertaining to interstate commerce regulation—including electronic information. In the absence of federal action, state action may be warranted. Yet that is not the case in data protection. From the Red Flag rules, to Gramm-Leach-Bliley, to SEC regulations, we should embrace federal standards as the ideal regulatory framework. Like Consumer Affairs did a few years ago on “Do Not Call” lists, compliance with one law should be seamless with the other and constitute compliance at both the federal and state level. Such a framework creates ease of compliance and education for the employer and consumer alike. A thorough Massachusetts comparison of these regulations with at least the FTC Red Flag Rules seems prudent and necessary at this point.

RAM Recommends: As permitted in the statute, the regulation should clarify that compliance with similar federal standards constitutes compliance with this regulation. At the same time care is necessary to ensure that the state standards do not exceed in requirement strength or costs of the federal standards. Otherwise certain small businesses which may not be regulated by the Red Flag rules or other existing federal standards could be harmed competitively by being required to follow a stricter state standard than existing federal regulations.

Encryption

No one doubts the importance of moving towards encrypted data when personally identifiable information is involved. Yet no one—large or small—can get there overnight. Small businesses, large businesses, non-profits, and taxpayer funded institutions, all purchase computer equipment, software, and point of sale systems as economics allow. New systems could certainly be encrypted, but not systems purchased even just a few years ago. For the state to require an immediate investment in totally new systems in order to fight criminal acts perpetuated against all of us, represents an unfair financial burden for any business, particularly in extremely difficult economic times.

Moreover, there is a difference between encrypting laptops and PCs so that information contained in files stored on laptops and PCs may not be accessed inappropriately and sending an individual email that is encrypted with a digital certificate so that the email is unreadable over the public network. The requirement of universal encryption of files transmitted over public networks or wirelessly presents special problems that no company, regardless of its size or resources can presently solve. Companies frequently communicate with their retail customers by e-mail, and those communications are likely to contain personal information. In order for encryption to work, each customer would have to apply compatible encryption software on their personal computer. It is simply not possible for different companies to require different encryption software of customers in order to communicate with them.

Furthermore, for credit card transactions, most small businesses use dial up terminals over phone lines. Although credit card transactions over the Internet are indeed encrypted, phone transactions are not, and don't need to be as they are completely secure.

RAM Recommends: *The encrypted data requirement should not have any deadline at all, but rather should be required on a going forward basis for any new investment, upgrade and or equipment purchase. Furthermore, flexibility should be allowed for other secure alternatives, and explicit exemptions should be given for otherwise secure transmissions over phone lines.*

Inventory Process

At first blush, one might think that this is an easy process. Not true. After internal education and a plan of action is developed—itsself a several month process—individuals, departments, auditors and consultants will need to work long and hard on this requirement.

RAM Recommends: *The inventory process should be delayed at least for one year until January 1, 2010.*

Third Party Service Providers

Many retailers, large and small, use third party vendors that hold personal information on their consumers or employees. Leased selling areas in stores, finance companies, extended warranty providers, home installation and repair companies, delivery companies, website providers, security system vendors, payroll companies, accountants, technical support and employee background screening companies are just a few of the examples of third party vendors that retailers may use.

Most large retailers have existing contracts with their vendors that will need to be revisited in order to obtain certification stating that they are in compliance with this regulation. This process may lead to a renegotiation of terms which may take months. Indeed, based on real-world experience, it could take years to obtain certification from all vendors. For example, one of our member companies has already initiated a process for requiring its vendors to contractually agree to certain security standards. That company has been negotiating over the inclusion of privacy policy language into an existing contract for more than a year with a very large, well-respected vendor who has excellent security policies. At a minimum, therefore, the certification requirement should be applied only to new or renewed contracts. It should not require companies to reopen existing contracts.

It has been suggested that most vendor and service provider contracts have clauses which automatically require compliance with any new applicable law, which would make this third party requirement easier. We have found that is not the case in many instances even for large companies, and certainly not so with small businesses where contracts are often slanted toward the provider or vendor.

Additionally, many small employers have existing contractual obligations with vendors that are located out of state. In many instances, the vendor may have an attorney on staff or may have hired an attorney to write and/or negotiate the contract while the small business did not have legal representation. Many of these contracts are governed by the laws of the state in which the vendor is located and may not give the consideration to changes in Massachusetts law. Therefore, instead of

complying with the Massachusetts regulation, a vendor may opt to terminate the contract thereby leaving a Massachusetts company at a disadvantage as they need to quickly negotiate a contract with a different vendor. Furthermore, many companies may need to hire legal representation to renegotiate or terminate existing contracts which will certainly be a financial burden on a small business. It is important to keep in mind the legal liability and potential financial loss to companies that are forced to terminate existing agreement.

RAM Recommends: *The certification of third party vendors requirement should only be required as new relationships are made, new contracts are written, or expiring contracts are renewed. Prior contracts and relationships should be grandfathered in.*

Applicability to Government Entities

Fully a third of all data breaches that have occurred over recent years were with government entities. During the debate on the original ID theft legislation, it was certainly the stated intention of the drafters that private employers should not be held to a different standard than public employers. If costly government mandates are not put on government entities as well—from cities and towns, to state government and federal government—then one must question both the importance of the intent of the regulation, and the fairness of the regulation.

RAM Recommends: *The regulation be clarified that it applies to all government entities at all levels holding personal information of Massachusetts residents.*

Applicability of 93A Enforcement Actions

It is our opinion that the authors of the legislation did not in any way want to put local employers at risk for private right of action under 93A. The existing regulation creates a question whether local companies will be put at very serious legal risks of bounty hunter legal actions any time a breach is reported to the state.

RAM Recommends: *The regulation should be clarified to limit enforcement solely to the Attorney General, and clarify that no private right of action exists under 93A.*

We sincerely ask you to consider the difficulties companies are facing and the reality of becoming compliant by May 1, 2009. The scope is enormous, especially as we recognize that identity theft is a crime that companies are diligently trying to prevent with different plans or action. Companies must be allowed adequate time to implement and carry out new procedures as outlined in this regulation in order to best protect their customers and employees' personal information.

Thank you for the opportunity to submit these comments and please feel free to contact us should you feel we can be of further assistance.

ROBERT A. PELOQUIN
PRESIDENT
CPCU, CIC, LIA, AAI, LUTC
NOTARY PUBLIC



408 OLD COLONY RD.
P. O. BOX U
NORTON, MA 02766-0947
VOICE: (508) 226-4076
FAX: (508) 226-6235

January 8, 2009

Good Old Fashioned Service

Daniel Crane, Undersecretary
David Murray, General Counsel
Office of Consumer Affairs & Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116



Top Priority: Protect Personal Information through Stakeholder Analysis

Dear Sirs:

As an employer with 3 employees, I am very concerned, about the mandates currently included in 201 CMR 17.00. As written, these regulations set a perilous course for my business, state agencies and our shared goals to invest and protect jobs in the Commonwealth. I urge the Patrick's Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 with the Department, Attorney General, regulated community and elected officials, to re-issue an entire set of rules by May 1, 2009 with implementation of the rules over a two year period.

As a business owner or employee the protection of personal information for residents of the Commonwealth is a top priority. The delay in the effective date is helpful, as a practical matter, it is unreasonable to believe that my firm has a fair opportunity to reach full compliance. As currently written, 201 CMR 17.00 goes beyond the legislature's intent and mandates specific technologies, creates redundant and confusing rules and does not hold public agencies to the same standards of the private sector. In many instances the regulatory mandates are not technically or economically feasible for public or private agencies regardless of size or available resources. Further, the regulations do not envision the national and global business relationships that the Massachusetts economy depends on.

The implications of 201 CMR 17.00 will have a negative impact on "all persons" and all firms that conduct business in Massachusetts. The promulgation and implementation of these specific regulations are in sharp contrast with other states and especially other Massachusetts state agencies that routinely engage in collaborative discussions with the regulated communities. The state of New Jersey recognized the need for a vigorous stakeholder analysis. Currently, the State of New Jersey is currently in a two year process just to promulgate a "pre-proposal" of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey's new pre-proposal provides for a comment period until February 13, 2009. Regrettably, the Massachusetts



regulations do not provide similar time, clarity, recognition of federal regulations nor do they recognize the significant technological, legal, operational challenges or the significant investments and human talent that many persons and small firms must now face.

The following is a partial list of the issues and solutions that the business community has identified:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules to achieve the ultimate goal of compliance. The regulations should be implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Otherwise the contract and written certification requirement becomes a never ending, complex, costly, and circular mandate virtually without end.

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute. A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology.

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated. A better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. The risk assessment approach would be similar to what is required in other federal and state contexts.

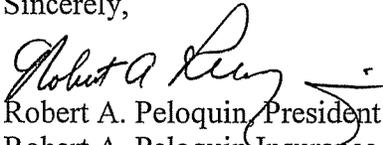
Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations. Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy

Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose

Under these rules "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 to "all persons" or firms, regardless of readily available resources.

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. Thank you for considering the long-term implications of these regulations and their direct impact on my business and the Massachusetts economy.

Sincerely,



Robert A. Peloquin, President
Robert A. Peloquin Insurance Agency, Inc.
408 Old Colony Road
PO Box U
Norton, MA 02766

**COMMENTS OF THE
SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)**

regarding

**“Promulgation of Amendments to 201 CMR 17.00: Standards for
the Protection of
Personal Information of Residents of the Commonwealth”**

(As provided in the Notice of Public Hearing, issued December 1, 2008)

January 15, 2009

On behalf of the members of the Software & Information Industry Association (SIIA), we appreciate this opportunity to submit our comments on the proposed amendments to regulation 201 CMR 17.00 implementing the provisions of Massachusetts General Law c. 93H, relating to the standards to be met to safeguard the personal information of residents of the Commonwealth of Massachusetts.

As the principal trade association of the software and digital information industry, the more than 500 members of SIIA develop and market software and electronic content for business, education, consumers and the Internet.¹ SIIA's members are software companies, ebusinesses, and information service companies, as well as many electronic commerce companies. Our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies.

SIIA commends the Massachusetts Department of Consumer Affairs and Business Regulation (DCABR) for holding the hearing on January 16, and for recognizing the time and costs associated with implementation of the unique approach taken by the Massachusetts regulations to implement safeguards for personal information. Our Association supports the proposed amendments to 201 CMR 17.00, which extends to January 1, 2010, the compliance date for obtaining a

¹ Our website can be found at www.sii.net.

certification from third party service providers,² and for encrypting portable devices other than laptops,³ and extends to May 1, 2009, the compliance date with respect to all other provisions of 201 CMR 17.00.

SIIA believes that this delay is an important, constructive step and an opportunity to review the practicality of the regulations *as a whole as promulgated*; in particular, the growing realization of the substantial costs to small, medium and large businesses of compliance with the regulations and the effects of the regulation in the context of other legal and regulatory requirements (including those imposed by other states and under federal law, as well as international obligations that entities must meet in the area of information security). SIIA remains concerned that, even with the delay, reconciling the implementation of the Massachusetts regulations with other legal obligations in other jurisdictions may not be feasible.

Growing Concern with Massachusetts' Disparate Approach

Even with the constructive changes incorporated into the final promulgated regulations issued last September, preparation for their implementation indicates that the mandated standards, at minimum, are far from co-existent with existing federal requirements for most businesses, and in some important respects, are likely to create disparate obligations from those imposed in other jurisdictions in the United States, even for those industries that are subject to specific regulation (such as financial and health care services).

For example, no other federal, state, or (to the best of our knowledge) other country's laws require encrypting personal information to such an extent, and with such specificity, as that found in the 201 CMR 17.00. By contrast, other obligations impose on entities the requirement that security protections must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the information it handles.⁴

The disparate approach is also confirmed by the requirements of the standards which differ from any other federal or US state law in establishing the requirement

² 201 CMR 17.03(f).

³ 201 CMR 17.04(5).

⁴ See, e.g., "Safeguards Rule" (Final Rule, "Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information", 16 C.F.R. Part 314 (published May 23, 2002). See also "Final Report of the Advisory Committee on Online Access and Security" (May 15, 2000), found at: <http://www.ftc.gov/acoas/papers/finalreport.htm#III>", Sec. 3.4.4. ("...adopt security procedures (including managerial procedures) that are 'appropriate under the circumstances.' 'Appropriateness' would be defined through reliance on a case-by-case adjudication to provide context-specific determinations.")

that a person must “limit ... the amount of personal information collected *to that which is reasonably necessary to accomplish the legitimate purpose for which it is collected.*” In a similar vein, the prescriptive regulatory limitation on “the time such information is retained to that reasonably necessary to accomplish such purpose” is not found in any other US statutory requirement, including those for highly regulated industries. And the prohibition to “limit... access to those persons who are *reasonably required to know such information in order to accomplish such purpose...*” is likewise unique to Massachusetts for otherwise non-regulated data under federal law.⁵

By way of final example, no other federal or state law requires a 3rd party to provide a separate certificate to a person that owns, licenses, stores or maintains personal information about others that it has a written, comprehensive information program *that is in compliance with a particular state or federal regulation.*⁶ This requirement not only imposes obligations upon the person that holds the data of Massachusetts’ residents but expands the requirement’s reach to require entities with no business in Massachusetts to follow all of the regulation’s technical and administrative requirements.

Cost and Business Impact is Significantly Underestimated

SIIA has carefully reviewed materials prepared by DCABR in the form of FAQ’s and guides via its website.⁷ We want to highlight several points regarding the assumptions and conclusions found under the “Fiscal Effect and Small Business Impact Statement.”⁸

SIIA recognizes -- indeed strongly advocates -- that investment in sound information security practices and technology is essential to any business that collects, maintains or uses sensitive personal information. Based on the experience of responsible entities that have sought to comply not only with existing legal obligations, but also good industry practices, the lesson learned is that the investment must be carefully thought through, as these investments are likely to be a noticeable and growing budget component of any entity’s operating costs.

⁵ See, for all three examples, 201 CMR 17.03(g) (italicized emphases added).

⁶ 201 CMR 17.03(f).

⁷ See “Identity Theft” webpage for Business, found at: <http://www.mass.gov/?pageID=ocatopic&L=3&L0=Home&L1=Business&L2=Identity+Theft&sid=Eoca>.

⁸ Found at: http://www.mass.gov/?pageID=ocaterminal&L=3&L0=Home&L1=Business&L2=Identity+Theft&sid=Eoca&b=terminalcontent&f=idtheft_sbimpact&csid=Eoca

Taking into account this experience and perspective, we have studied the cost assumptions outlined by the DCABR and find that those assumptions significantly underestimate the cost and complexity of compliance with the promulgated regulations for small, medium and large businesses. According to the website FAQ, “increased costs may include the costs of new or updated versions of software,” but that “many businesses may simply need to activate security features in hardware and software that is already in place on their computer systems or networks.” DCABR assumes as context a 10-person business; but, even in the case of larger businesses, the DCABR asserts that they “will already have in place all the resources and management support necessary for compliance, and therefore will experience little fiscal impact associated with compliance.” As described in more detail below, the technological, operational and administrative burdens associated with implementing these unique regulations belie the assumptions found in the DCABR notice.

The website FAQ describes a hypothetical analysis involving a small business and concludes that the “up-front cost ... should not exceed \$3,000, with ongoing technical oversight, monitoring and maintenance that would likely be absorbed within currently existing technical support program.” For those entities where no such technical support currently exists, the required support to comply with the detailed Massachusetts regulations “should cost no more than \$500 per month.” The website FAQ goes on to assert that “much of the software needed for such a company to comply with [the regulations] is available as free software.”

While the hypothetical analysis is not exactly clear on the point, these factors appear to be relevant to implementation of only part of the new standards, in particular Section 17.04 (related to Computer System Security Requirements). We note, however, that the website FAQ’s lack any careful delineation of how *activating security features in already existing hardware and software* meets all eight of the prescriptive elements listed in Section 17.04 or otherwise satisfies an entity’s legal exposure, even to inadvertent violations of the standards. Moreover, SIIA is not aware of any ‘system’ that is widely used by (or available generally off-the-shelf for) many small and medium-sized businesses that, by ‘mere activation’, implements each and every one of elements 1-8 of Section 17.04.

By way of just one example, it is highly unlikely that hardware or software systems that are currently available provide for “mere activation” of built-in features that would facilitate all of element (5), in particular “encryption of all personal information on ... other portable devices” (beyond laptops), particularly at the corporate or business administrator level. As a further example, in order to address the encryption *and monitoring* requirements alone, meaningful investment in necessary infrastructure and technology will be required by most companies.

More significantly, the cost estimates underlying the Notice of proposed amendments, and the Website FAQ’s are limited to only section 17.04 and do not take into account the substantial resources required to fulfill Section 17.03 (Duty to

Protect and Standards for Protecting Personal Information). That section includes both development and implementation of an information security plan by every person that owns, licenses, stores or maintains personal information, as well as certification of each 3rd party service provider that might access such personal information *prior* to the person permitting such access to the 3rd party. Those requirements, among many, require the designation (which will necessitate on-going training) of one or more employees and the development of security policies for all employees.

Based on our understanding of efforts to develop such plans in other regulatory contexts, and review of efforts to begin to comply with the Massachusetts regulations, the development of such plans can be as costly (if not more expensive) than the deployment of technology that facilitates the secure maintenance and use of personal information.

As outlined earlier in our comments, regarding the particular ways in which the Massachusetts regulations are unique from other Federal, state and many international obligations, ***even an entity that has had to comply with federal laws requiring an on-going written security plan⁹ may not simply rely on any such plan as a ‘safe harbor’ or necessarily a ‘reasonable’ effort to comply with Section 17.04***, since the State’s standards include many key elements that go beyond those outlined in federal rules.

The requirement that 3rd parties provide a certification that they have a “written, comprehensive information security program that is in compliance with the provisions of these regulations” – which may or may not be related to the 3rd party’s handling of the personal information owned, licensed, stored or maintained by the contracting person -- is inconsistent with the requirements of other laws, which focus on contractual obligations “flowing down”. This has implications not just for small businesses – where the hypothetical \$500 per month technical support person must provide such certification – but also for medium and larger size entities which will be required to re-negotiate contracts with dozens, indeed hundreds, of supplier and partners globally.

Efforts by medium and larger companies to comply may require significant reworking of existing enterprise architectures and databases, which do not as a practical matter segregate customers and other business partners from whom sensitive personal information may be collected based on location.

SIIA continues to look forward to working with the DCABR as it reviews the public record. We would be glad to answer any questions or try to provide additional information that might be helpful.

⁹ See “Safeguards Rule”.

January 21, 2009

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

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

Dear Mr. Murray:

The State Privacy and Security Coalition and the National Business Coalition on E-Commerce and Privacy (“Coalitions”) appreciate the opportunity to share our views regarding the extension granted by the Office of Consumer Affairs and Business Regulation (OCABR) with respect to effective dates for certain aspects of 201 CMR 17.00, *Standards for the Protection of Personal Information of Residents of the Commonwealth*.

The State Privacy & Security Coalition consists of the nation’s leading Internet Service Providers (ISPs), technology companies, and technology trade associations, who have significant operations in and outside the Commonwealth of Massachusetts. The National Business Coalition on E-Commerce & Privacy is a deliberately diversified organization of brand name companies and associations, including financial services and manufacturing companies with significant operations in and outside the Commonwealth of Massachusetts.

The Coalitions appreciate the OCABR’s recognition of the significant regulatory challenges created by the data security regulations, and, in particular, the requirements to (1) obtain certifications from third service providers that such entities are complying with the OCABR’s data security regulations and (2) encrypt the personal information of Massachusetts residents both in storage and in transit.

The Coalitions, however, continue to harbor strong misgivings about the OCABR’s assertion of rulemaking authority under the statute. The Coalitions believe that the OCABR has exceeded its authority under the statute and is impermissibly regulating interstate commerce in violation of the Commerce Clause of the U.S. Constitution. If it intends to enforce the data security regulations at all, however, the Coalitions respectfully request that the OCABR consider a longer extension of time - until January 1, 2011 - to facilitate full compliance with the regulations.

I. Legal Authority to Promulgate Data Security Regulations

A. The OCABR Has Exceeded its Authority to Promulgate Data Security Regulations Under the Authorizing Statute

Under the authorizing statute, the OCABR is directed to issue regulations that are “designed to safeguard the personal 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.” MASS. GEN. LAWS ch. 93H, § 2(a)(emphasis added). The regulations acknowledge this statutory directive, noting that businesses are to implement a comprehensive information security program with safeguards that “*must be consistent* with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns, licenses, stores or maintains such information may be regulated.” 201 MASS. CODE REGS. § 17.03 (emphasis added).

Although some aspects of the OCABR’s data security regulations are similar to the Gramm-Leach-Bliley (GLB) Safeguards Rule *see, e.g.*, 16 C.F.R. § 314, which also serves as the *de facto* data security standard for businesses that are not subject to federal data security rules, other portions of the proposed regulations, including the third party certification and encryption requirements, significantly deviate from the GLB Safeguards Rule. The prescriptive nature of these requirements are inconsistent with both the language and the spirit of the GLB Safeguards Rule.

Although Massachusetts courts generally grant deference to regulations promulgated by an administrative agency, which are entitled to a presumption of validity, “principles of deference...are not principles of abdication.” *Nuclear Metals, Inc. v. Low-Level Radioactive Waste Mgt. Bd.*, 421 Mass. 196, 211 (1995). “When an agency’s interpretation of its regulation cannot be reconciled with the governing legislation, that interpretation must be rejected.” *Id.* Under Massachusetts law, an administrative agency “has no authority to promulgate rules and regulations which are in conflict with the statutes or exceed the authority conferred by the statutes” under which the agency operates. *Duarte v. Commissioner of Revenue*, 451 Mass. 399, 411 (Mass. 2008) (internal citations and quotations omitted); *see also Massachusetts Mun. Wholesale Elec. Co. v. Massachusetts Energy Facilities Siting Council*, 411 Mass. 183, 194 (1991).

The Coalitions believe that the OCABR’s regulations cannot be reconciled with the authorizing statute, which directs the OCABR to promulgate regulations that are “consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated.” MASS. GEN. LAWS ch. 93H, § 2(a). The prescriptive nature and broad reach of the OCABR’s regulations strongly militate, at the very least, toward an additional extension of time, particularly in light of the OCABR’s departure from the authorizing statute in promulgating the data security regulations.

B. The Data Security Regulations Violate the Commerce Clause of the U.S. Constitution

The data security regulations require, “[t]o the extent technically feasible, encryption of all transmitted records and files containing personal information, including those in wireless environments, that will travel *across public networks*.” 201 MASS. CODE REGS. § 17.04(3)(emphasis added). Additionally, the regulations require “[e]ncryption of all personal information stored on laptops or other portable devices.” § 17.04(5). Separate provisions that require companies to identify (and effectively inventory) all records containing “personal information” about Massachusetts residents and require third party service providers in possession of “personal information” about Massachusetts residents to certify compliance with the OCABR’s data security regulations raise similar constitutional concerns.

The Commerce Clause of the U.S. Constitution provides that “Congress shall have power...[t]o regulate Commerce...among the several States.” U.S. CONST. art. I, § 8, cl. 3. The

negative implication of the Commerce Clause prohibits states from regulating commerce that impermissibly burdens interstate commerce. See *Lewis v. BT Inv. Managers, Inc.*, 447 U.S. 27, 35 (1980) (“Although the Clause thus speaks in terms of powers bestowed upon Congress, the Court long has recognized that it also limits the power of the States to erect barriers against interstate trade.”).

The “Dormant Commerce Clause” prohibits two distinct form of state regulation that impermissibly burden interstate commerce – (1) protectionist laws that discriminate against commerce from other states in favor of the enacting state and (2) state regulations that, although facially nondiscriminatory, unduly burden interstate commerce. See e.g. *Kassel v. Cons. Freightways Corp. of Del.*, 450 U.S. 662 (1981).

Even where a state regulates in an evenhanded fashion to achieve a legitimate local interest, the law will nevertheless violate the Dormant Commerce Clause if “the burden imposed on such commerce is clearly excessive in relation to the putative local benefits.” *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970). Where a legitimate local purpose can be articulated, “then the question becomes one of degree.” *Id.* A state statute that burdens interstate commerce will be invalidated in this context if the legitimate local purpose “could be promoted as well with a lesser impact on interstate activities.” *Id.* Under these circumstances, the Court embraces a “balancing approach” to determine whether a state regulation impermissibly burdens interstate commerce.” *Id.*

The borderless nature of the Internet makes commercial Internet communications inextricably intertwined with interstate commerce. The Supreme Court has recognized that “[t]he internet is ‘a unique and wholly new medium of worldwide human communication’located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.” *Reno v. ACLU*, 521 U.S. 844, 850-51 (1997).

Courts have been receptive to Dormant Commerce Clause challenges to state laws that impermissibly burden *Internet* commerce. See e.g. *PSINet v. Chapman*, 362 F.3d 227, 240 (4th Cir. 2004) (“Given the broad reach of the Internet, it is difficult to see how a blanket regulation of Internet material...can be construed to have only a local effect.”); *ACLU v. Johnson*, 194 F.3d 1149, 1161 (10th Cir. 1999) (stating that a New Mexico statute did not contain a limitation of its reach to in-state conduct and therefore constituted “an attempt to regulate conduct outside New Mexico’s borders, and is accordingly a per se violation of the Commerce Clause.”); *American Libraries Ass’n v. Pataki*, 969 F.Supp. 160, 168-69 (S.D.N.Y. 1997) (“The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed.”).

By its very nature, the Internet is an interstate means of communication. In *Pataki*, the court observed that “[t]he Internet is wholly insensitive to geographic distinctions,” *id.* at 170, and opined that “no aspect of the Internet can feasibly be closed off to users from another state.” *Id.* at 171. The court thus opined that “[t]he inescapable conclusion is that the Internet represents an instrument of interstate commerce, albeit an innovative one; the novelty of the technology should not obscure the fact that regulation of the Internet impels traditional Commerce Clause considerations.” *Id.* at 173. *Pataki* overturned a New York state law that restricted the display of content on the Internet because it (1) regulated conduct occurring outside of New York’s borders;

(2) subjected the interstate use of the Internet to conflicting regulations; and (3) imposed burdens on interstate commerce that exceeded any local benefit.

In *Johnson*, the Tenth Circuit overturned a New Mexico law prohibiting the dissemination of harmful material to a minor by computer. The court observed that “the Supreme Court has long recognized that certain types of commerce are uniquely suited to national, as opposed to state, regulation.” *Johnson*, 194 F.3d at 1160. The proscription at issue in *Johnson* contained no express limitation confining the statute’s reach to communications that occurred wholly within New Mexico’s borders. *Id.* at 1161. The court thus concluded that the law “represents an attempt to regulate interstate conduct occurring outside New Mexico’s borders, and is accordingly a per se violation of the Commerce Clause.” *Id.*

Although it held that the law in *Johnson* constituted a *per se* violation of the Commerce Clause, the Tenth Circuit also held that the law impermissibly burdened interstate commerce under the *Pike* balancing test. The court opined that the burdens on interstate commerce exceeded any putative local benefits served by the statute. *Id.* While New Mexico successfully articulated a compelling governmental interest in enacting this law, the court asserted that the constitutional validity of this provision rests on “whether the means chosen to further that interest excessively burden interstate commerce compared to the local benefits the statute actually confers.” *Id.* at 1161. Additionally, the court sought to underscore the inconsistent regulation that persons and entities would be subject to as a result of the law’s enforcement. *Id.* at 1162.

The OCABR’s data security regulations violate Dormant Commerce Clause principles in at least two ways.

First, in requiring “encryption of all transmitted records and files containing personal information, including those in wireless environments, that will travel across public networks,” the regulations unambiguously regulate commerce that occurs substantially (if not wholly) outside of Massachusetts’s borders. Moreover, as discussed in more detail below, by mandating encryption, Massachusetts has also cast aside technology neutrality and asserted instead a State preference for one form of technology over many others that render data “unusable”. This choice only serves to exacerbate the burden on interstate commerce that occurs outside the Commonwealth.

As the Fourth Circuit observed in *PSINet*, it is difficult to conceive of a blanket regulation of Internet commerce that has only a local effect. Like the statute at issue in *Johnson*, the encryption requirement, which applies to all personal information “that will travel across public networks”, is not expressly limited to transmissions of personal information that occur in Massachusetts. The encryption requirement unambiguously implicates activity that largely occurs beyond Massachusetts’s borders.

Indeed, there are many scenarios where the encryption requirement will regulate commercial activity that occurs wholly beyond Massachusetts’ borders. A third party service provider that is based in Illinois, for example, may transmit personal information about a Massachusetts resident “across public networks” to a health insurance company that is located in California. The encryption requirement, however, chooses one form of technology over another and regulates this transmission of personal information, and additionally regulates the information security practices of the third party service provider, despite only an attenuated nexus to Massachusetts.

It is difficult to overstate the likely impact that the data security regulations will have on interstate commerce. Many companies and third party service providers that maintain personal information about Massachusetts residents, but otherwise have no connection to Massachusetts, are likely unaware of the OCABR's data security regulations, and will have to expend significant resources in order to comply with the regulations. The encryption requirement is by no means limited to Massachusetts; entities located in other states will be subject to the encryption requirements if they maintain personal information on a single Massachusetts resident. Any business that reaches a broad audience of consumers and that relies on the efficient flow of information will be impacted by the extremely broad reach of the OCABR's data security regulations.

Second, the goals of the data security regulations could be effectuated through a less prescriptive approach that would have commensurate benefits for Massachusetts residents. Such an approach would have the added benefit of faithfully adhering to the Legislature's directive, which instructed the OCABR to craft regulations consistent with those promulgated in federal regulations by functional regulators. The OCABR can promulgate data security regulations that enhance protections for Massachusetts residents without substantially and adversely affecting interstate commerce. The GLB Safeguards Rule is a lodestar for a flexible regulatory approach that would have a minimal impact on interstate commerce. Because any tangible benefits of the OCABR's data security regulations for Massachusetts residents are uncertain, a prescriptive approach that burdens interstate commerce likely implicates Dormant Commerce Clause principles.

II. Substantive Concerns about the Data Security Regulations

A. Third Party Certification Requirement

The data security regulations provide that "prior to permitting third-party service providers access to personal information, the person permitting such access shall obtain from the third-party service provider a written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of these regulations." 201 MASS. CODE REGS. § 17.03(f).

The third party certification requirement appears to apply to both new *and* existing contracts and/or relationships with third party service providers. Applying this requirement to existing contractual relationships between businesses and service providers, however, will have unintended consequences that will likely redound to the detriment of Massachusetts consumers, as well as increase both administrative and legal expenditures for businesses that are already facing an extremely difficult economic climate. Although some contracts include change of law provisions that may effectively resolve potential disputes between businesses and third party service providers, not all contracts include such provisions. Indeed, many contracts between businesses and third party service providers lack such provisions. Additionally, some contracts that do have change of law provisions actually release third party service providers from performance in the event of a change of law.

The requirement to obtain a separate certification from third party service providers that they are in compliance with a state-specific regulatory scheme is inconsistent with the GLB Safeguards Rule. Pursuant to the GLB Safeguards Rule, the Federal Trade Commission (FTC) merely requires certain financial institutions to oversee service providers by "[t]aking reasonable steps to select and

retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue [and]...[r]equiring your service providers by contract to implement and maintain such safeguards.” 16 C.F.R. § 314.4(d)(1-2).

Delaying the effective date of the third party certification requirement until January 1, 2010, is a step in the right direction. The Coalitions, however, urge the OCABR to revisit the third party certification requirement altogether. At the very least, the third party certification requirement should only be applied to new (and not existing) contracts in order to both facilitate compliance with this requirement and avoid disrupting existing business relationships in a manner that could adversely affect Massachusetts residents.

B. Encryption Requirements

The Coalitions continue to believe that it is unwise to freeze any particular technological standard into law. Encryption is not a panacea. Technology will inevitably advance. Although encryption is a strong data security protocol in some circumstances, there are drawbacks to its utilization. The widespread usage of encryption throughout an enterprise can significantly slow traffic across public networks, which reduces efficiency and strains bandwidth. This is particularly true with public key encryption, which tends to be cheaper, and thus is more likely to be used by businesses that are covered by the encryption mandate. Encryption keys can also be lost or compromised. Under such a scenario, the underlying data can be extremely difficult, if not impossible, to recover.

The process of equipping non-portable and portable devices with encryption is labor-intensive, time-consuming, and expensive. Encrypting files that contain personal information and that are transmitted across public networks is even more problematic, since it would require any recipients of the encrypted communication to obtain compatible software in order to read encrypted files. The costs of any encryption requirement imposed by the OCABR, therefore, would be borne not only by Massachusetts businesses, but also by any entity that receives personal information about Massachusetts residents.

The drawbacks associated with encryption favor a flexible approach that allows businesses to choose from a variety of data protection methods that are capable of protecting the security and confidentiality of personal information. This flexible approach is what the Massachusetts Legislature envisioned in directing the OCABR to promulgate regulations consistent with those issued under federal regulations. The Coalitions accordingly request the OCABR to permit businesses to choose from a wide variety of data protection methodologies that are capable of protecting the security and confidentiality of personal information.

C. Identifying Records Containing Personal Information

The proposed regulations required the “inventorying” of records that contain personal information about Massachusetts residents. The final regulations provide that a component of the written information security program must include “*identifying* paper, electronic, and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to identify those records containing personal information.” 201 MASS. CODE REGS. § 17.03(h)(emphasis added).

In practical terms, there is no material difference between an information security program requirement that entails the identification of records that contain personal information and an information security program requirement that entails the inventorying of records that contain personal information. Despite the use of the word “identifying” in Section 17.03(h), the language of the rule suggests the inventorying of all records that contain personal information. The process of identifying records in this context inevitably entails the inventorying of documents that contain personal information.

A comprehensive inventory of all written and electronic records that contain personal information would be extraordinarily burdensome. Moreover, such a requirement will not directly or appreciably enhance the security and confidentiality of personal information. It is unclear, for example, precisely how this requirement should be implemented. Is it sufficient that businesses merely create a log identifying documents that contain personal information? Alternatively, does this particular requirement further envision that businesses will classify any and all data that contains personal information? Further guidance is necessary to clarify how the OCABR expects businesses to implement this requirement.

With respect to paper documents, many large organizations store vast amounts of information at offsite locations. Moreover, many electronic documents that contain personal information have been imaged into databases. Section 17.03(h) would require such electronic documents to be un-imaged, even if the underlying personal information contained in the document was already secure. Requiring businesses to sift through documents at offsite warehouses or in electronic databases for the sole purpose of complying with this requirement is neither practical, nor a useful allocation of data security resources.

III. Conclusion

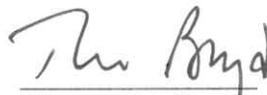
The Coalitions appreciate the OCABR’s willingness to extend the effective dates of the data security regulations. The uncertain legal validity of the OCABR’s actions, coupled with the significant disruptions that could be wrought by requiring compliance with the data security regulations, militates, at the very least, toward a delay until January 1, 2011.

Thank you for your time and consideration.

Sincerely,



David A. Lieber
Counsel to the State
Privacy and Security Coalition



Thomas M. Boyd
Counsel to the National Business
Coalition on E-Commerce and Privacy



January 15, 2009

Via Electronic Mail

Mr. David Murray
General Counsel
Office of Consumer Affairs and Business Regulation (OCABR)
Ten Park Plaza, Suite 5170
Boston, MA 02116

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

Dear Mr. Murray:

Symantec Corporation appreciates the opportunity to submit our comments on regulation 201 CMR 17.00 implementing the provisions of General Law c. 93H, relating to the standards to be met to safeguard the personal information of residents of the Commonwealth of Massachusetts.

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec supports voluntary encryption that utilizes our industry's best practices and widely adopted standards. We believe that states should provide incentives for implementation of encryption technology, rather than mandating the use of that or any particular technology. Furthermore, we believe that 201 CMR 17.00 places undue burdens on Massachusetts businesses, and others attempting to do business in the commonwealth, and for that reason respectfully recommend that OCABR further revise the regulations. To that end, we strongly support the attached comments submitted by the Software & Information Industry Association (SIIA), of which Symantec is a member of the Board of Directors.

However, upon any further review OCABR still chooses to mandate the use of encryption technology, Symantec takes the position that the commonwealth should adopt an internationally recognized standard such as FIPS - 140, which is widely accepted according to our technology experts. Our experts also assert that there already exists interoperability of standard encryption technologies.

We appreciate OCABR's willingness to address outstanding concerns with industry stakeholders. Thank you for your time and consideration of our comments. We would be pleased to answer any questions or provide any further information you or your staff may need. Please do not hesitate to contact me directly at either 703-283-0347 or owen_sweeney@symantec.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Owen M. Sweeney, Jr.", written in a cursive style.

Owen M. Sweeney, Jr.
State Government Relations

Technology Association of America



AeA NEW ENGLAND COUNCIL

444 Washington Street
Woburn, MA 01801-1072
Tel. 781.938.1925 Fax 781.938.0091
Visit our web site at: www.aeanet.org/NewEngland

**STATEMENT OF THE
TECHNOLOGY ASSOCIATION OF AMERICA (AeA and ITAA)
BEFORE THE MASSACHUSETTS OFFICE OF
CONSUMER AFFAIRS AND BUSINESS REGULATION
IN CONNECTION WITH
201 CMR 17.00 -- STANDARDS FOR THE PROTECTION OF PERSONAL
INFORMATION OF RESIDENTS OF THE COMMONWEALTH**

Good afternoon.

My name is Anne Doherty Johnson and I am the Executive Director of AeA New England. AeA has merged with ITAA as of January 1, 2009 forming the Technology Association of America and is the nation's largest high technology trade association representing over 1,350 high tech companies.

We would like to thank Secretary O'Connell and Undersecretary Crane and the Massachusetts Office of Consumer Affairs and Business Regulation for calling this hearing and for the opportunity to share comments regarding 201 CMR 17.00. This is an important issue, and we also thank you, the Legislature, Attorney General Coakley and the Patrick Administration for their continued attention to this matter.

AeA member companies are committed to protecting sensitive personal information from identity theft — a goal that the private and public sectors equally share. AeA also recognizes that there is a role for well-crafted and meaningful legislation and regulations in advancing this goal.

We commend the Administration for delaying the implementation of 201 CMR 17.00. This was a necessary first step to allow our member companies to identify the costs and other significant logistical and practical problems associated with attempting to comply with these far-reaching regulations. However, a delay alone is not enough. Our companies have spent significant time working on compliance and continue to have serious concerns. Some requirements are technically problematic, potentially extremely costly, and, in many cases, impractical. As a result, they would have serious unintended consequences for all entities -- including companies of all sizes, non-profit organizations and individuals -- who do business with Massachusetts residents. We therefore ask that the OCABR consider substantively amending the regulations to address their more egregious aspects.

(continued)

AeA suggests four ways in which the regulations could be significantly improved. These suggestions are the result of many hours of discussion and review with our member companies, who have in turn spent many hours and dollars trying to decide how best to deal with the regulations.

First, Section 17.04(3) would obligate companies to encrypt “all transmitted records and files containing personal information that will travel across public networks” and to encrypt “all data to be transmitted wirelessly” unless “technically infeasible.” Subsection (5) of this same provision also would obligate companies to encrypt “all personal information stored on laptops or other portable devices.”

The regulations incorrectly assume that encryption technology (including the necessary state-of-the-art computer hardware, operating systems and application software) is readily available to all organizations and individuals and that it is reasonably straightforward to encrypt information on all types of portable media and wireless transmissions. The regulations fail to recognize that while certain encryption technologies do exist, they are evolving, there is no universally accepted standard, the diverse systems are often not mutually interoperable, and these technologies are not in all cases readily available to, and certainly not widely deployed or used by, businesses, organizations and individuals in Massachusetts or elsewhere in the industrialized world.

Second, the definition of “Encryption” in Section 17.02 of the regulations is a flawed definition because it leaves open the possibility of future changes without input from the affected industries. In addition, the phrase “at least as secure” is unclear since there is not a defined standard for what “secure” means.

AeA has put forward a definition supported by the technology community and adopted in 30 other states that encourages the development of future technological breakthroughs that could better protect data elements. It also has the benefit of being technology neutral and would provide incentives to using best available technologies to achieve the intended result, such as storage of data elements in separate databases, which are often more effective or more cost-effective protection than encryption.

Third, the third party service provider regulation in Section 17.03(f) would, in many cases, require the renegotiation of all service contracts, the creation of new internal procedures, and both internal and external education and training. These requirements, in turn, would potentially be quite costly. Affected Persons would be forced to stop doing business with any counterparty unable to provide these certifications on a timely basis, creating market disruption for customers and potential delays to the products and services on which they depend. These requirements also exceed the authority of the Commonwealth since they require companies outside the jurisdiction of the state to comply.

(continued)

Fourth, the inventory requirement in Section 17.03(h) would be an unprecedented obligation and extraordinarily time consuming and expensive, to the extent that it is feasible at all. Many companies and institutions would have to hire consultants or staff specifically for this project, resulting in significant upfront costs as well as recurring maintenance costs to keep the documentation up-to-date.

Massachusetts is the only state to have regulations as wide-reaching as these and has also gone forward without adequately listening to any of the technology industry's concerns. New Jersey is the only other state that has implementing regulations to accompany their identity theft legislation and in stark contrast to what has happened here in Massachusetts, they have taken a far more measured and deliberative approach, by first issuing pre-proposed regulations and including representatives from technology and other sectors throughout their decision making process.

As a major technology state, we owe it to the state's consumers to do a better job at crafting regulations that are workable and duly protect data. AeA strongly encourages the Office of Consumer Affairs and Business Regulation to work with the technology industry to address the implementation and definitional challenges these regulations represent. We look forward to helping you address this challenge. I can be reached at 781.938.1925, x105. Thank you.

Joe Zukowski
Vice President – Government Affairs



185 Franklin Street Room 1703
Boston, MA 02110

Phone: 617-743-1278
Fax: 617-743-8881
joseph.h.zukowski@verizon.com

January 15, 2009

Daniel C. Crane, Undersecretary
Office of Consumer Affairs and
Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116

**Re: 201 CMR 17.00 - Standards for the Protection of
Personal Information of Residents of the Commonwealth**

Dear Undersecretary Crane:

Verizon shares the concerns of the Associated Industries of Massachusetts and a wide range of businesses and industries regarding the proposed regulations in 201 CMR 17.00. As I testified late last year before the Joint Committee on Consumer Protection, Verizon currently complies with many of the new regulations due to the substantial policies and procedures we already have in place to protect the confidential information of our customers and employees.

I write separately, however, to highlight some issues of particular concern to Verizon and to ask that you amend the regulations or provide us with written guidance that confirms our view of reasonable compliance. Where we make specific clarifications to the regulations, I have attached a markup of 201 CMR 17.00 indicating such changes.

Encryption (17.02). The definition of “encrypted” is overly narrow. Subsection 17.02 defines “encrypted” as “the transformation of data through the use of an algorithmic process, or an alternative method at least as secure.” Tunneling-mode encryption secures the path over which data is transmitted, rather than encrypting the data itself, but in Verizon’s view is at least as secure as data encryption. It also has the advantage of protecting the data without requiring Verizon or its vendors to change their data storage, entry and retrieval systems, thereby allowing us to operate more efficiently than if the data were encrypted. Verizon therefore asks for a clarification that “encryption” includes the use of tunneling-mode encryption as well.

Third Party Vendor certification (17.03(f)). In its letter to you of October 15, 2008, AIM explained why the regulation should explicitly state that electronic statements from vendors are sufficient for compliance. Verizon agrees that such clarification is appropriate, and that electronic documents satisfy the regulation, in light of the provisions of M.G.L. c. 110G, §§ 7 and 9. In addition, the regulation should clarify that vendors who merely pass personal information on to their client and do not retain access to that data need not certify that they too have implemented a program in conformance with the rules, since the need for such a program is minimal where the vendor retains neither the data nor access to it.

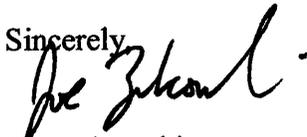
Identifying paper, electronic and other records (17.03(h)). Verizon has policies in place to identify all such databases and systems and to protect against the improper disclosure of personal information. This regulation could be misread, however, to require an inventory or identification of *every single* paper or electronic record that contains personal information. This regulation should clearly exempt small listings or compilations of personal information used in day-today business functions.

Reviewing the scope of security measures annually or upon a material change in business practices (17.03(k)). Verizon makes use of more than 700 software systems to conduct its business. Because the substantive requirements of 220 CMR 17.00 are so broad, much broader for example than federal requirements regarding CPNI, subsection 17.03(k) arguably could require Verizon to review annually the security measures in place with respect to these 700+ systems, an enormous task. The security measures Verizon has in place are not affected by the change of a calendar year, making the requirement of an annual review unreasonable and needlessly expensive. Verizon suggests that the regulation or its interpretation be clarified to require reviews only upon a material change in business practices that implicates the security or integrity of databases or other compilations of records that contain personal information.

We also note that the final clause of rule 17.04(3), which requires “encryption of all data to be transmitted wirelessly,” is not limited to personal information. It is therefore both beyond the authority of the Office of Consumer Affairs to promulgate regulations under Chapter 93H and is unnecessary, since there is no valid public policy reason to require businesses to encrypt non-personal information, including public information, that is transmitted wirelessly.

We appreciate the efforts your office has made to listen to the concerns of the business community, and would ask that you give full consideration to these suggestions.

Sincerely,



Joe Zukowski
Vice President – Government Affairs
Verizon

Cc: Sen. Michael Morrissey, Joint Committee on Consumer Protection
Rep. Michael Rodrigues, Joint Committee on Consumer Protection

201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth

Section:

17.01: Purpose and Scope

17.02: Definitions

17.03: Duty to Protect and Standards for Protecting Personal Information

17.04: Computer System Security Requirements

17

17.01 Purpose and Scope

(a) Purpose

This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. Further purposes are to (i) ensure the security and confidentiality of such information in a manner consistent with industry standards, (ii) protect against anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud against such residents.

(b) Scope

The provisions of this regulation apply to all persons that own, license, store or maintain personal information about a resident of the Commonwealth.

17.02: Definitions

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

"Breach of security", the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

"Electronic," relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

"Encrypted," ~~(i) the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key or (ii) the use of tunneling-mode encryption or an equivalent thereof to secure the path over which data is transmitted.~~

Deleted: , unless further defined by regulation by the office of consumer affairs and business regulation

"Person," a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

"Personal information," a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"Record" or "Records," any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

17.03: Duty to Protect and Standards for Protecting Personal Information

Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information. Such comprehensive information security program shall be reasonably consistent with industry standards, and shall contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records. Moreover, the safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns, licenses, stores or maintains such information may be regulated.

Whether the comprehensive information security program is in compliance with these regulations for the protection of personal information, whether pursuant to section 17.03 or 17.04 hereof, shall be evaluated taking into account (i) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program, (ii) the amount of resources available to such person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information. Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

- (a) Designating one or more employees to maintain the comprehensive information security program;
- (b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to: (i) ongoing employee (including temporary and contract employee) training; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures.
- (c) Developing security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.

(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

(e) Preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.

(f) Taking reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information, including (i) selecting and retaining service providers that are capable of maintaining safeguards for personal information; and (ii) contractually requiring service providers to maintain such safeguards. ~~After January 1, 2010, prior to permitting third-party service providers access to personal information, the person permitting such access shall obtain from the third-party service provider a written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of these regulations. Such written certification may be in electronic form. This subsection 17.03(f) shall not apply to a third-party service provider that receives either a credit or debit card number for payment purposes or a social security number for a credit check and subsequently transmits that information to the person on whose behalf the information was received where the third-party does not retain that information (other than temporarily in the active memory of a computer) and has no access to that information in or from the systems of the party to whom the numbers were transmitted.~~

Deleted: P

(g) Limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limiting the time such information is retained to that reasonably necessary to accomplish such purpose; and limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements.

(h) Identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information. ~~This subsection 17.03(h), however, shall not apply to small listings or compilations of personal information, such as emails or handwritten notes, used and retained on a short-term basis in the ordinary course of business.~~

(i) Reasonable restrictions upon physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and storage of such records and data in locked facilities, storage areas or containers.

(j) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

(k) Reviewing the scope of the security measures ~~whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.~~

Deleted: at least annually or

(l) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

17.04: Computer System Security Requirements

Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, shall have the following elements:

- (1) Secure user authentication protocols including:
 - (i) control of user IDs and other identifiers;
 - (ii) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
 - (iii) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
 - (iv) restricting access to active users and active user accounts only; and
 - (v) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
- (2) Secure access control measures that:
 - (i) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
 - (ii) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
- (3) To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all personal information to be transmitted wirelessly. Deleted: data
- (4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
- (5) Encryption of all personal information stored on laptops or other portable devices, provided that such person shall have until January 1, 2010 to encrypt personal information on such other portable devices;
- (6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
- (7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
- (8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

17.05: Effective Date

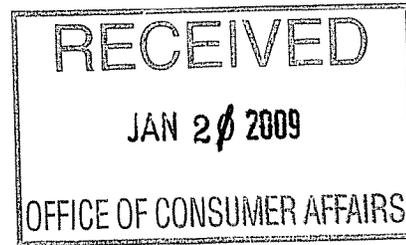
Every person who owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall, unless otherwise expressly provided herein, be in full compliance with 201 CMR 17.00 on or before May 1, 2009.

Deleted: January

Formatted: Font: **Bold, Underline**

REGULATORY AUTHORITY:

201 CMR 17.00: M.G.L. c. 93H



Peter L. McCorkell
Senior Company Counsel

Law Department
45 Fremont Street
27th Floor
MAC A0194-277
San Francisco, CA 94105
Phone: 415-396-0940
Fax: 415-975-7863

Via Federal Express

January 20, 2009

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

**RE: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE
COMMONWEALTH, 201 CMR 17.00**

Ladies and Gentlemen:

Wells Fargo & Company and its subsidiaries, including the Wachovia companies acquired by Wells as of December 31, 2008, appreciate the opportunity to comment on the Standards for the Protection of Personal Information of Residents of the Commonwealth adopted as 201 CMR 17.00 (the "Regulations"). The combined Wells Fargo/Wachovia enterprise is one of the largest financial services organizations in the United States and includes commercial banks, a consumer finance company, trust and asset custody operations, insurance agents, brokers and underwriters, and securities broker-dealers and investment and funds managers. Evergreen Investments, based in Boston, the world's first family of mutual funds, has offered investment services and products since 1932 and is now part of the Wells Fargo/Wachovia family of companies.

Virtually all of our businesses either have customers who are residents of Massachusetts or serve other businesses whose customers include residents of Massachusetts. Those same businesses have customers who reside in other jurisdictions; in many cases, they have customers who reside in all fifty states as well as countries other than the United States. Information about those customers is, for the most part, stored and processed in centralized data systems, and not segregated by the jurisdictions in which those customers happen to reside. In order to provide efficient and effective protection of customer information, Wells Fargo utilizes corporate level policies and procedures that apply across the enterprise.

It should be noted that these businesses are “financial institutions” subject to the data security standards and guidelines adopted by various federal regulatory agencies pursuant to Section 501(b) of the federal Gramm-Leach-Bliley Act (15 U.S.C. Section 6801(b), hereafter referred to as “GLBA”). These federal standards have been in place since 2001 and require our businesses to “implement a comprehensive written information security program... appropriate to the size and complexity of the [institution] and the nature and scope of its activities.” E.g., Appendix B to 12 CFR Part 364B. Most of our businesses are not only subject to these federal requirements, but are regularly examined by federal regulatory agencies for compliance with these obligations. The statute mandating adoption of the Regulations recognized the value of ensuring that they be “consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated.” M.G.L. c. 93H, sec. 2(a).

In contrast to the results-oriented, risk-based approach taken in the data security standards and guidelines adopted by the federal financial regulatory agencies (and other states, such as New Jersey), the Massachusetts Regulations contain many very detailed prescriptive requirements. We believe that, in many cases, complying with these specific requirements would impose significant additional costs and constraints on businesses that have customers who reside in the Commonwealth, without producing any real benefit in terms of additional security for those Massachusetts residents. If other jurisdictions chose to adopt information security requirements that are equally prescriptive but which differ in detail from those adopted by Massachusetts, nation-wide and international businesses may well be faced with redundant or even conflicting requirements.

Accordingly, we urge you to revise some of the most onerous aspects of the Regulations to be less prescriptive and more risk-based and results-oriented. Alternatively we would urge adopting a provision that would recognize compliance with federal laws, regulations or guidelines regarding the safeguarding of personal information as constituting compliance with the Commonwealth’s regulations. Finally, if certain aspects of the Regulations are retained without modification – in particular certification of compliance by service providers – we would urge that businesses be given additional time to come into full compliance.

SPECIFIC PROVISIONS OF THE REGULATIONS

SERVICE PROVIDER CERTIFICATIONS; 201 CMR 17.03(f)

Perhaps the most onerous provision now in the Regulations is the requirement that every business obtain a separate, unqualified certification from every “service providers” with access to personal information that the service provider is in full compliance with the Regulation. Service providers with only minimal ties to Massachusetts will be understandably reluctant to provide such a certification since it requires them to be conversant with Massachusetts law and regulations, and in many cases may require them to adopt specific practices which are unnecessary and cost-prohibitive. At least in the financial services arena, service providers have already been required to enter into written agreements with respect to information security applicable on a national basis, so they can be expected to resist what they perceive to be a redundant requirement, especially if it may be only the first of 50 (or more) such certifications covering the various States and perhaps foreign jurisdictions. Alternatively, such service

providers may use the request for a separate certification as an opportunity to renegotiate contract terms, thus placing additional stress on an already strained financial services system.

Obtaining such certifications would be a massive undertaking. For example, just one of our more than 100 business units has in excess of 2,000 "service providers" from which, under federal rules, it is required to obtain written assurance of compliance with federal information security requirements. Multiply that figure by the tens or hundreds of thousands of businesses with Massachusetts customers who rely on "service providers" and the certifications will create a blizzard of paperwork which, in and of itself, provides not an iota of additional protection for Massachusetts residents. Diligence in selecting and overseeing service providers and appropriate contractual provisions provide the real protection, and clearly satisfy the underlying statute's call to safeguard customer information in a manner fully consistent with industry standards. M.G.L. c. 93H, sec. 2(a). Accordingly, we urge that the last sentence be deleted from Section 17.03(f).

Also, there is a real "chicken and egg" problem with such certifications: a service provider that is dependent on one or more subcontractors cannot honestly certify that it is in full compliance until it has received certifications from each of those subcontractors. The GLBA rules cited above already require financial institutions to obtain "written agreement" from service providers with access to personal information that they have an adequate information security program. Such provisions are usually part of the contract between the institution and the service provider, rather than a separate certification. We urge you to make it clear that agreements which satisfy the GLBA rules will be deemed to satisfy the written certification requirement of the Regulations.

In addition, there are a number of issues around the scope of the term "service provider" that should be clarified. First, it should be made clear that businesses are required to obtain a written agreement or certification only from service providers with whom the business has a direct contractual relationship as defined by GLBA. Utilization of the GLBA definitions would facilitate consistency with the rigorous safeguarding rules to which financial institutions are already subject. Second, one business should not be considered a "service provider" if it has an independent relationship with the customer. For example, an investment fund may distribute its products through broker-dealers who might be considered "service providers" to the fund. However, the consumer has a separate and direct relationship with the broker-dealer, so it and not the fund should be directly responsible for securing the consumer's information in its control. Finally, it should be made clear that government agencies will never be considered "service providers" subject to this requirement, since the reality is that private businesses cannot control how government agencies protect information and almost certainly will never be able to obtain agreements or certifications from them in this regard.

ENCRYPTION OF PORTABLE DEVICES; 201 CMR 17.04(5)

The requirement to encrypt all "portable devices" which contain personal information, if absolute, may be impossible to satisfy. It is possible to safeguard portable storage media by means other than encryption, and it may not be technically feasible to encrypt some types of storage media. Indeed, rather than prescribing encryption, Section 17.04(5) of the Regulations should be modified to require "appropriate measures be taken to safeguard personal information

on portable devices from unauthorized access” and that encryption be treated as a possible but not exclusive way to satisfy that requirement. Regulation should focus on the goal of preventing unauthorized access to personal information instead of prescribing a specific technical approach. Requiring a specific methodology for protecting data may impair the ability of businesses to adopt new technologies that may prove more effective than the prescribed approach.

INVENTORYING OF RECORDS; 201 CMR 17.03(h)

Some businesses – and probably many government agencies – may find it virtually impossible to complete a thorough inventory of all records containing “personal information” by the May 1, 2009, deadline, or to ever have a truly comprehensive inventory. Implementation of a comprehensive information security program, protecting all personal information wherever it may be located, would adequately protect such information, and thus should obviate the need for such an inventory.

LIMITATIONS ON THE COLLECTION AND RETENTION OF INFORMATION; 201 CMR 17.03(g)

As currently written, the Regulations require that collection of personal information be limited “to that reasonably necessary to accomplish the legitimate business purpose for which it is collected” and that such information be retained only for as long as required “to accomplish such purpose.” We are concerned that the use of the singular terms “the..purpose” and “such purpose” might be construed to prohibit “secondary” uses of data, a result which has no basis in the underlying statute and which clearly exceeds the scope of these data security Regulations. Information collected primarily for one purpose is frequently used for other purposes, often referred to as a “secondary” use. In the financial services industry, information obtained when a consumer applies for one product or which is obtained in the course of servicing one product is often used to suggest other products that may provide value to the consumer. For example, the fact that a particular customer occasionally overdraws a checking account but has generally good credit might be used to offer the customer a credit card account with overdraft protection, thus saving the customer from the expense and inconvenience of dishonored checks. Our concern regarding “secondary use” could be addressed by changing the language of this section to read, in part: “Limiting the amount of personal information collected to that reasonable necessary to accomplish legitimate business purposes; limiting the time such information is retained to that reasonably necessary to accomplish such purposes;...”

COMPLIANCE DEADLINES; 201 CMR 17.05

Federally regulated financial service providers subject to the GLBA requirements are probably much closer to compliance with the Regulations than most other types of businesses simply because we have been subject to the federal rules for many years. But because we have significant real-world experience in implementing such requirements, we are acutely aware of the time and resources required to design and implement comprehensive information security programs, even when detailed, prescriptive requirements are not mandated. Especially if the service provider certification and encryption requirements are not modified, we urge you to delay the mandatory compliance date for at least those portions of the Regulations at least an additional 12 months, to January 1, 2011.

January 20, 2009

CONCLUSION

Wells Fargo and Wachovia appreciate the opportunity to comment on the Regulations. Please feel free to contact the undersigned at (415) 396-0940 or mccorkpl@wellsfargo.com if you have any questions regarding the foregoing comments.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter J. McCorkle". The signature is written in a cursive style with a large initial "P" and "M".