

201 CMR: OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION

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
- 17.05: Compliance Deadline

17.01: Purpose and Scope

(1) Purpose. 201 CMR 17.00 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. 201 CMR 17.00 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:

- (a) ensure the security and confidentiality of such information in a manner consistent with industry standards;
- (b) protect against anticipated threats or hazards to the security or integrity of such information; and
- (c) 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.

(2) Scope. The provisions of 201 CMR 17.00 applies to all persons who own, license, store or maintain personal information about a resident of the Commonwealth.

17.02: Definitions

The following words as used in 201 CMR 17.00 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.

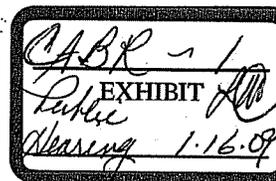
Electronic, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted, 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, 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



17.02: continued

(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

(1) Every person who 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.

(2) Whether the comprehensive information security program is in compliance with 201 CMR 17.00 for the protection of personal information, whether pursuant to 201 CMR 17.03 or 17.04, shall be evaluated taking into account:

- (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;
- (b) the amount of resources available to such person;
- (c) the amount of stored data; and
- (d) 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:

1. Designating one or more employees to maintain the comprehensive information security program;
2. 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:
  - a. ongoing employee (including temporary and contract employee) training;
  - b. employee compliance with policies and procedures; and
  - c. means for detecting and preventing security system failures.
3. 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.
4. Imposing disciplinary measures for violations of the comprehensive information security program rules.
5. 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.
6. Taking reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information, including:
  - a. selecting and retaining service providers that are capable of maintaining safeguards for personal information; and
  - b. 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 201 CMR 17.00.

17.02: continued

7. 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.
8. 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.
9. 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.
10. 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.
11. Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
12. 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 who 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:
  - (a) control of user IDs and other identifiers;
  - (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
  - (c) 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;
  - (d) restricting access to active users and active user accounts only; and
  - (e) 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:
  - (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
  - (b) 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 data to be transmitted wirelessly.
- (4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;

17.04: continued

(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: Compliance Deadline

Every person who owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall, unless otherwise expressly provided in 201 CMR 17.00, be in full compliance with 201 CMR 17.00 on or before May 1, 2009.

REGULATORY AUTHORITY

201 CMR 17.00: M.G.L. c. 93H.



**COMMONWEALTH OF MASSACHUSETTS  
OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION**

10 Park Plaza - Suite 5170, Boston MA 02116  
(617) 973-8700 FAX (617) 973-8799  
TTY/TDD (617) 973-8790  
www.mass.gov/consumer

DEVAL L. PATRICK  
GOVERNOR

TIMOTHY P. MURRAY  
LIEUTENANT GOVERNOR

DANIEL O'CONNELL  
SECRETARY OF HOUSING AND  
ECONOMIC DEVELOPMENT

DANIEL C. CRANE  
UNDERSECRETARY

**NOTICE OF PUBLIC HEARING**

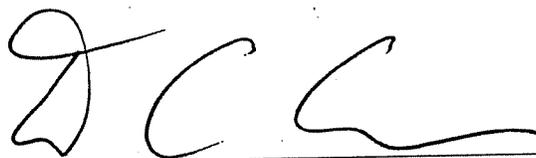
Pursuant to the provisions of M.G.L. c. 30A, and to the authority granted to the Director of the Office of Consumer Affairs and Business Regulation pursuant to M.G.L. c. 93H, the Office of Consumer Affairs and Business Regulation will hold a public hearing in connection with the promulgation of amendments to 201 CMR 17.00 that extend the date for compliance with the provisions of those regulations as originally promulgated. These amended regulations were previously promulgated as emergency regulations on November 14, 2008. The public hearing will commence at 2:00 p.m. on Friday, January 16, 2009, in Room No. 5-6, Second Floor of the Transportation Building, 10 Park Plaza, Boston, Massachusetts 02116.

The purpose of the public hearing is to afford interested parties an opportunity to provide oral or written testimony regarding the aforementioned amendments to 201 CMR 17.00, *Standards for the Protection of Personal Information of Residents of the Commonwealth*. Those amendments extend to January 1, 2010 the compliance date for obtaining a certification from third party service providers pursuant to 201 CMR 17.03(f), and for encrypting portable devices other than laptops pursuant to 201 CMR 17.04(5), and extend to May 1, 2009 the compliance date with respect to all other provisions of 201 CMR 17.00.

Interested parties will be afforded a reasonable opportunity at the hearing to present oral or written testimony. Written comments will be accepted up to the close of business on Wednesday, January 21, 2009. Such written comments may be mailed to: Office of Consumer Affairs and Business Regulation, 10 Park Plaza, Suite 5170, Boston, MA, 02116, Attention: David A. Murray, General Counsel, or e-mailed to [David.Murray@state.ma.us](mailto:David.Murray@state.ma.us).

Copies of the proposed regulation may be obtained from the Office of Consumer Affairs and Business Regulation website [www.mass.gov/oca](http://www.mass.gov/oca) ; or by calling (617) 973-8700.

December 1, 2008

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

2008 DEC - 1 PM 3:00  
SECRETARY OF STATE  
REGULATIONS DIVISION

CABR-2  
EXHIBIT  
Public Hearing - 1-16-09



**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](http://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.

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

Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052-6399

Tel 425 882 8080  
Fax 425 936 7329  
<http://www.microsoft.com/>

**Microsoft**

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.

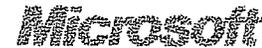
Microsoft fully supports the goals behind the regulations and Massachusetts statute, and we recognize the need to create safeguards to protect the personal information of Commonwealth residents. We have a long-standing commitment to data security in our own products. Microsoft's Office Outlook<sup>®</sup> 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.



- The regulation of third party service providers under §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. Since a large number of the technical controls specified in the regulation are impossible to comply with in the short term, and some are just not commercially or technically feasible, it is likely that no entity will be able to comply with all aspects of §17.03(f). It will not be possible, therefore, to receive the certifications required by this provision. Affected companies would be forced to stop doing business with third parties that are 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. This will have a disproportionate impact on small businesses that are least likely able to certify compliance and they may lose vital revenue as a result.
- The physical control requirements stated in §17.03 (i) mandate the storage of records and data in locked facilities. However, this type of control is only applicable in centralized computing environments like data centers and would not be reasonable to deploy for such devices as laptops for mobile users, portable storage devices, SmartPhones, etc. Other types of mitigating controls would be appropriate in such circumstances. This is one of the many mandated controls in the regulation that do not offer the flexibility of applicability; this control should only be used when it is applicable and feasible. The regulation offers no flexibility to substitute reasonable alternative technical or procedural controls. The stringency of the control should also scale with the risk; safeguarding a single record of personal information requires a different investment than safeguarding hundreds of thousands of records. The prescriptive language of the regulation does not offer the flexibility scale controls commensurate with the risk.

Microsoft fully supports the Commonwealth's intent to protect the personal information of its residents. We have made significant investments in product innovation to help our own customers address these concerns. The rapid evolution to Internet based computing has created, and continues to create, new threats that require a variety of responses. Our operational experience proves that allowing companies to invest in the most appropriate controls by "taking into account (i) the size, scope and type of business" is the best approach. This approach leaves the decision of which technical controls to deploy, to those who know best how to assess and address the risk.

Sincerely,

A handwritten signature in black ink that reads "Steven Michalove / SN".

Steven Michalove, CISM, CISSP

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

Informational Hearing on November 19<sup>th</sup> 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](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](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](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.



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. Stewart & Sons  
Company, Inc.

**Vice Chairman**

Larry E. Mulvey  
Foodmaster Supermarkets

**Secretary**

Thomas R. Zapf  
Mays

**Treasurer**

Howard M. Honigbaum  
Ann Sand 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 Berni

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.

**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 17<sup>th</sup>, 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 19<sup>th</sup>, I testified before the Legislature's Joint Committee on Consumer Protection and Professional Licensure regarding our concerns with the rules. On November 26<sup>th</sup>, at the request of the Department as a follow-up to our November 17<sup>th</sup> 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 12<sup>th</sup>, 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 24<sup>th</sup> identified each of the issues from our November 26<sup>th</sup> 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 17<sup>th</sup>, 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 1<sup>st</sup> 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 1<sup>st</sup> 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 1<sup>st</sup>. 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 1<sup>st</sup> and January 1<sup>st</sup>, 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.

---

# 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.

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.



---

91 Cedar Street, Milford, MA 01757  
TEL (508) 634-2900 ■ (800) 972-9312 ■ FAX (508) 634-2929  
Francis A. Mancini, Esq., President & CEO



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.

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.

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.<sup>1</sup> AIM has communicated with thousands of Massachusetts businesses and has provided hundreds of Massachusetts employers with education and resources through webinars<sup>2</sup> and seminars<sup>3</sup> 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

---

<sup>1</sup> 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.

<sup>2</sup> AIM provided four webinars

<sup>3</sup> 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.<sup>4</sup> 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

---

<sup>4</sup> 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.

**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.

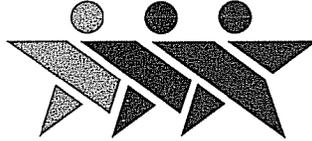
Accordingly, we do not believe these regulations were written to cover this sector in its relationship to state government and believe it should be exempt.

#### **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.



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).

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;

- 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.

**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.



11 Beacon Street, Suite 1224 | Boston, Massachusetts 02108-3093  
617.742.5147 | FAX 617.742.3089 | [www.masscolleges.org](http://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.

### 3<sup>rd</sup>-Party Verification

The 3<sup>rd</sup>-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 3<sup>rd</sup>-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 3<sup>rd</sup>-party vendor. If that 3<sup>rd</sup>-party vendor then enters into a subsequent transaction with a different vendor the 3<sup>rd</sup>-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**

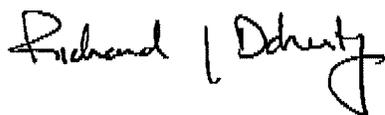
Many colleges and universities use a "point card" system that essentially allows a student to use his/her Student ID card as a declining balance card to make purchases on campus. A student deposits money into an account and then uses his/her ID card to redeem "points" in exchange for books, food, and 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

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.

**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 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 form 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,



Marylou Buyse, M.D.  
President



## 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.

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.

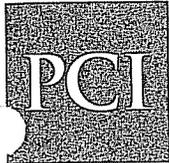
In addition, we are hopeful that the Office of Consumer Affairs and Business Regulation will clarify that, if the requirement is not eliminated, certification from third party vendors is required only once as well as provide a definition for the term "portable device."

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



**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, reading "Francis C. O'Brien", is written over a large, light-colored scribble or stamp.

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.

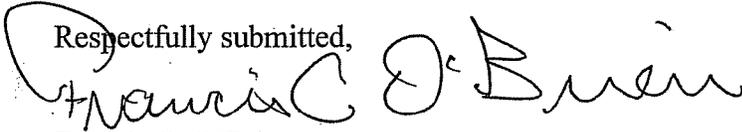
• ***Overly Rigid Standard of Encryption.*** The enabling statute defines “encrypted” as “transformation of data through the use of a 128-bit or higher algorithmic process into a form *in which there is a low probability of* assigning meaning without use of a confidential process or key. . . .” G.L. 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 21<sup>st</sup> 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

**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. 93H<sup>1</sup> with respect to standards for the protection of personal information of Massachusetts residents.

---

<sup>1</sup> 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. (Sec. 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.

Pages: 1-92  
Exhibits: 1-2  
Written Submissions: 17

**COMMONWEALTH OF MASSACHUSETTS**

**CONSUMER AFFAIRS and BUSINESS REGULATION**

**PUBLIC HEARING**

**201 CMR 17.00**

PUBLIC HEARING in connection with the promulgation of **201 CMR 17.00** concerning **Standards for the Protection of Personal Information of Residents of the Commonwealth**, taken pursuant to the applicable provisions of Massachusetts General Laws before Lindsey A. Cyr, a Notary Public and Court Reporter in and for the Commonwealth of Massachusetts, at the **Transportation Building**, Room 5-6, Second Floor, 10 Park Plaza, Boston, MA, 02116 on **Friday, January 16, 2009**, commencing at **1:56 p.m.**

---

**CYR ASSOCIATES**  
Postal Box 22  
North Weymouth, MA 02191  
781-337-4638

## A P P E A R A N C E S

David A. Murray, Hearing Officer/General Counsel  
**Office of Consumer Affairs & Business Regulation**  
 10 Park Plaza - Suite 5170  
 Boston, MA 02116

---

## S P E A K E R I N D E X

	<u>Page</u>
Opening of Hearing	6
Anne Doherty Johnson, Executive Director <b>AeA New England Council</b>	10
Mark E. Schreiber, Esquire <b>EDWARDS ANGELL PALMER &amp; DODGE, LLP</b>	16
Jon B. Hurst <b>Retailers Association of Massachusetts</b>	23
Tami Salmon <b>Investment Company Institute</b>	31
Daniel J. Foley, Jr. <b>Massachusetts Association of Insurance Agents</b>	44
Bradley A. MacDougall Assoc. V.P. Government Affairs <b>Associated Industries of Massachusetts</b>	51
Attorney Andrea Cramer <b>HIRSCH ROBERTS WEINSTEIN -- AIM</b>	52

	3
Michael Ripple Providers' Council	61
Jack Daniel Internet & Network Security Vendor	64
Mary Ann Clancy Massachusetts Credit Union League, Inc.	70
Timothy Sweeney Great Boston Chamber of Commerce	73
Robert McCarin AICUM	81
Gerry Hammon Newbury College	87

----

### E X H I B I T S

<u>No.</u>	<u>Description</u>	<u>Page</u>
1	Copy of Amended 201 CMR 17.00: Standards for the Protection of Personal Information of Resi- dents of the Commonwealth; 4 pages	6
2	Copy of Notice of Public Hearing pursuant to M.G.L. Chapter 30A and the authority granted to the Director of the Office of Consumer Affairs and Business Regulation under M.G.L. Chapter 93H, 1 page	9

---

**W R I T T E N   S U B M I S S I O N S**

Statement of Anne Doherty Johnson, Executive Director, **Technology Association of America (AeA and ITAA)**; and Statement on **Stakeholder Analysis - Protect Personal Information**

Letter on letterhead of **Microsoft**, dated January 15, 2009 addressed to Undersecretary Daniel Crane and David Murray, signed by Steven Michalove, CISM, CISSP; and, Testimony for the Joint Committee on Consumer Protection & Professional Licensure by Steven Michalove, Principal Security Strategist

Testimony of **Retailers Association of Massachusetts**, by Jon B. Hurst, President

Testimony of the **Investment Company Institute** by Tami Salmon

Statement of **Massachusetts Association of Insurance Agents** delivered by Daniel J. Foley, Jr., Vice President of Government Affairs and General Counsel

Statement of **Associated Industries of Massachusetts** delivered by Bradley A. MacDougall, Associate Vice President for Government Affairs

Letter on letterhead of **Providers' Council for Caring Communities** delivered by Michael Ripple

Statement of **Massachusetts Credit Union League, Inc.** delivered by Mary Ann Clancy

Statement of **Greater Boston Chamber of Commerce** delivered by Timothy Sweeney

Letter on letterhead of **Associated of Independent Colleges and Universities in Massachusetts - AICUM**, dated January 16, 2009, signed by Richard Doherty, President; and, read into the record by Robert McCarin

Document entitled: **Testimony; Massachusetts High Technology Council**

Statement of David E. Floreen, Senior Vice President, **Massachusetts Bankers Association**

Letter on the letterhead of **Massachusetts Association of Health Plans**, addressed to Daniel C. Crane, Undersecretary; signed by Marylou Buyse, M.D., President

Testimony of Bill Vernon, State Direct, **National Federation of Independent Business**

Letter on the letterhead of **Life Insurance Association of Massachusetts**; addressed to Daniel C. Crane, Director, Office of Consumer Affairs and Business Regulation; signed by Andrew J. Calamare, President and Chief Executive Officer

Letter on the letterhead of **Property Casualty Insurers Association of America - PCI**, signed by Francis C. O'Brien, Vice President, Regional Manager and Counsel with Statement attached

Statement of **American Insurance Association**

## P R O C E E D I N G S

1  
2  
3 HEARING OFFICER DAVID A. MURRAY: Can we get  
4 started, please.

5 The Hearing will come to order! I think  
6 it's close enough to 2 o'clock.

7 My name is David Murray. I'm the  
8 General Counsel of the Office of Consumer Affairs and  
9 Business Regulation; and, I am the Hearing Officer for  
10 this Public Hearing that's convened in connection with  
11 certain Amendments to 201 CMR 17.00 that were filed  
12 with the Secretary of State's Office on an emergency  
13 basis and became effective on November 14th of last  
14 year.

15 Copies of the Amended Regulation are at  
16 the table -- at the Speaker's Table.

17 [EXHIBIT ONE, being a copy of  
18 Amended Regulation is entered into  
19 the record]

20 This is a Public Hearing held pursuant  
21 to Chapter 30A of the General Laws, the Amendments to  
22 201 CMR 17 that are the subject of this Hearing and to  
23 which any offered testimony should be directed relate  
24 to the deferment of certain compliance dates.

1           The general compliance date was extended  
2 as a result of the Amendments from January 1st of this  
3 year to May 1st of this year; and, the compliance  
4 deadline for certain encryption requirements and for  
5 certain obligations in connection with the use of third  
6 party service providers were extended from January 1,  
7 2009 to January 1, 2010.

8           Notice of this Public Hearing was  
9 published in the Massachusetts Register on November  
10 28th, 2008 and in the Boston Globe on December 8, 2008;  
11 and, the Public -- the Notice of Public Hearing reads  
12 as follows:

13                           Pursuant to the provisions of  
14 Mass. General Laws, Chapter 30A,  
15 and to the authority granted to the  
16 Director of the Office of Consumer  
17 Affairs and Business Regulation  
18 pursuant to General Laws, Chapter  
19 93H, the Office of Consumer Affairs  
20 and Business Regulation will hold a  
21 public hearing in connection with  
22 the promulgation of Amendments to  
23 201 CMR 17.00 that extend the date  
24 for compliance with the provisions

1 of those regulations as originally  
2 promulgated.

3 These Amended Regulations were  
4 previously promulgated as Emergency  
5 Regulations on November 14th, 2008.

6 The hearing will commence at 2  
7 p.m. on Friday, January 16th, 2009  
8 in Room Nos. 5 and 6, Second Floor  
9 of the Transportation Building, 10  
10 Park Plaza.

11 The purpose of the public  
12 hearing is to afford interested  
13 parties an opportunity to provide  
14 oral or written testimony regarding  
15 the aforementioned Amendments to  
16 201 CMR 17.00.

17 Those Amendments extend to  
18 January 2010, the compliance date  
19 for obtaining a certification from  
20 third party service providers  
21 pursuant to 201 CMR 17.03(f) and  
22 for encrypting portable devices  
23 other than laptops pursuant to 201  
24 CMR 17.04, Sub (5); and, extend to

1 May 1, 2009 the compliance date  
2 with respect to all other  
3 provisions of 201 CMR 17.00.

4 Interested parties will be  
5 afforded a reasonable opportunity  
6 at the hearing to present oral or  
7 written testimony; and, written  
8 comments will be accepted up to the  
9 close of business on Wednesday,  
10 January 21st, 2009.

11 Such written comments may be  
12 mailed to the Office of Consumer  
13 Affairs, to my attention; and,  
14 copies of the Amended Regulations,  
15 as I said before, are either on the  
16 Speaker's Table here or you can  
17 obtain them from me if there aren't  
18 enough copies.

19 [EXHIBIT TWO, copy of Notice of  
20 Public Hearing was entered into the  
21 record.]

22 ---

23 As I hope everyone knows by now, there  
24 is a Sign Up Sheet at the table -- the Speaker's Table;

1 and, anyone wishing to testify at the Hearing must sign  
2 in on the Speaker's Sheet; and, for the benefit of the  
3 Stenographer, those testifying should spell their last  
4 names when introducing themselves.

5 If there are any elected officials who  
6 wish to testify, we will follow tradition and take them  
7 first.

8 [No Response]

9 So, let's get started with the Speakers.

10 I'd ask everyone to attend to their  
11 cellphone, please.

12 First on the list, Anne Doherty Johnson.

13 ---

14 **Anne Doherty Johnson**

15 **AeA New England Council**

16 Good afternoon! My name is Anne Doherty  
17 Johnson. I'm the Executive Director of AeA New  
18 England.

19 AeA, formerly the American Electronics  
20 Association, has merged with ITAA as of January 1, 2009  
21 forming the Technology Association of America and is  
22 the Nation's largest high tech trade association  
23 representing over 1350 high tech companies.

24 We want to take this opportunity to

1 thank, you, Secretary O'Connell and Undersecretary  
2 Crane, the Mass. Office of Consumer Affairs for calling  
3 the Hearing and for the delay in these Regulations.

4 This is an important issue. We, also,  
5 thank the Legislature, Attorney General Coakley and the  
6 Patrick Administration for their continued attention to  
7 this matter.

8 As you can see by the crowded room, we  
9 think more dialogue is needed.

10 AeA member companies are committed to  
11 protecting sensitive personal information from ID  
12 theft, a goal that the private and public sectors  
13 equally share. We recognize that there is a role for  
14 well-crafted and meaningful legislation and regulations  
15 in advancing that goal.

16 We commend the Administration for the  
17 delay. This is really a necessary first step to  
18 continue the dialogue; and, I'm going to be brief in my  
19 comments today because I'm sure you see there are a lot  
20 of -- of people that -- that want to weigh in on the  
21 issue.

22 We are part of a broad-based business  
23 coalition that has a number of suggestions for  
24 improving and streamlining and making these much more

1 workable for both Consumers and the Business Community.

2 AeA suggests four (4) ways in which the  
3 Regulations could be significantly improved. And,  
4 these are the results of continued discussions and --  
5 hours of discussion and review with our leading  
6 technology company members.

7 First, Section 17.04 would obligate  
8 companies to encrypt all transmitted records and files  
9 containing personal information that will travel across  
10 public networks and to encrypt all data to transmitted  
11 wirelessly unless technically infeasible.

12 Subsection (5) also would obligate  
13 companies to encrypt all personal info on laptops or  
14 other portable devices.

15 The Regulations incorrectly assume that  
16 encryption technology, including the necessary state-  
17 of-the-art computer hardware, operating systems and  
18 application software, is readily available to all  
19 organizations and individuals and that it is reasonably  
20 straightforward to encrypt information on all types of  
21 portable media and wireless transmissions.

22 The Regulations fail to recognize that  
23 while certain encryption technologies do exist, they're  
24 evolving; there are no universally accept standard; the

1 diverse systems are often not mutually inoperable --  
2 inter-operable; and these technologies are not, in all  
3 cases, readily available and not widely deployed or  
4 used by businesses, organizations and individuals in  
5 Massachusetts or elsewhere in the industrialized World,  
6 in fact.

7           Second, the definition of "Encryption"  
8 in Section 17.02 of the Regulations is a flawed  
9 definition; it leaves open the possibility of future  
10 changes without input and the phrase "at least as  
11 secure" is unclear since there is not a defined  
12 standard for what "secure" means.

13           We've put forward a definition supported  
14 by the technology community and adopted in other States  
15 that addresses some of these issues and we'd love to  
16 revisit that particular issue.

17           Third, the Third-Party Service Provider  
18 Regulation in Section 17.03 -- And, I'm sure you'll  
19 hear a lot about that from other parties; so, I'll be  
20 brief. -- we think continues to be non-workable. It  
21 requires a re-negotiation of all service contracts, the  
22 creation of new internal procedures, internal/external  
23 education and training which would be costly and very  
24 impractical in the real world at present.

1 Fourth, the inventory requirement in  
2 Section 17.03 would be an unprecedented obligation and  
3 extraordinarily time consuming and expensive, to the  
4 extent that it is feasible at all.

5 Bottom line, Massachusetts is the only  
6 State to have Regulations as wide-reaching as these and  
7 has also gone forward without adequately listening to  
8 all of the technology industry's and, in fact, business  
9 industry concerns.

10 New Jersey is the only other State that  
11 has Implementing Regulations to accompany their ID  
12 Theft Legislation; and, in stark contrast to what's  
13 appeared here, they've taken a far more measured and  
14 deliberative approach by first issuing pre-proposed  
15 regulations, including representatives from all  
16 impacted stakeholders in that process and having,  
17 really, a long term look in terms of implementation.

18 As a major technology State, we owe it  
19 to the State's Consumers to do a better job at crafting  
20 these Regulations making them workable and truly to  
21 protect data.

22 We strongly encourage the Office of  
23 Consumer Affairs and Business Regulation to continue to  
24 work with the business community, the technology

1 industry and others so we can improve this and get it  
2 right.

3 Also, at this time, I would like to  
4 present written comments from one (1) of our members,  
5 Microsoft; so, I have written comments as well; so, I  
6 won't take much more of your time.

7 But, we are very anxious and willing to  
8 continue to dialogue.

9 We think that improvements can be made.  
10 We have a number of workable solutions that you'll hear  
11 from members of the business coalition that we're  
12 engaged in and we continue to work to get it right in  
13 the weeks to come.

14 HEARING OFFICER MURRAY: Thanks.

15 And, you -- you have the written --

16 ANNE DOHERTY JOHNSON: Yes, I do.

17 HEARING OFFICER MURRAY: Thanks.

18 ANNE DOHERTY JOHNSON: And, that's a cover  
19 letter from Microsoft as well. Okay?

20 HEARING OFFICER MURRAY: Okay. Thank you.  
21 Thank you.

22 Mark Schrieber?

23 MARK SCHREIBER: Thank you, David.

24 ---

1                                   **Mark E. Schreiber, Esquire**

2                                   **EDWARDS ANGELL PALMER & DODGE, LLP**

3                                   My name is Mark Schreiber, S-C-H-R-E-I-  
4 B-E-R. I chair the Edwards & Angell, Palmer & Dodge  
5 Privacy Group, along with Peter Lefkowitz who is here  
6 from Oracle.

7                                   I co-chair the Privacy Committee at the  
8 Boston Bar Association.

9                                   I'm also co-chair for Privacy Matters of  
10 the World Law Group, an International affiliation of  
11 some 50 large law firms in 40 Countries.

12                                   I'm not here to testify, however, on  
13 behalf of any group, entity or any client.

14                                   You have and will hear numerous  
15 objections as to why these Regulations are defective,  
16 unworkable or, perhaps, impossible to comply with by  
17 May 1 and/or why they should be extended further.

18                                   I'm not here to reiterate any of those  
19 objections.

20                                   If these Regs are going to go into  
21 effect as they appear they are by May 1, I do have  
22 several observations and comments by one who works  
23 frequently in this field and interacts almost on a  
24 daily basis with companies trying to comply with these

1 Regs.

2 As we know, these are probably the most  
3 severe and robust Regulations of this sort in the  
4 Country. That may not have been the intended  
5 consequence.

6 We know that the Statute said that you  
7 had to write Regs and the Regs were deliberated at some  
8 length; but, that is the consequence.

9 With that consequence comes, I believe,  
10 a certain amount of responsibility to be able to make  
11 these Regulations work and work by May 1 or whatever  
12 subsequent dates are available.

13 To do that or what I mean by making the  
14 Regulations work are several factors:

15 One, a number of companies are not aware  
16 these Regulations even exist.

17 I would wager that one (1) out of a  
18 hundred, maybe one (1) out of a thousand companies in  
19 Massachusetts are aware of these Regs or that they're  
20 supposed to be developing programs to adhere to them.

21 The fact that, in this room, we,  
22 probably, four (4) times as many people as there were  
23 last January when we had the original testimony and  
24 Hearing reflects that.

1                   So, what's the implication of that?  
2           More outreach. I think the Agency needs to publicize  
3           these existence of the Regs better on radio or other  
4           media, schedule meetings on its own with Industry  
5           Organizations, whatever outreach mechanisms you can do,  
6           probably, will be worthwhile because having created  
7           this Reg with the scope that it now entails, there's a  
8           lot of work to be done by a lot of companies, many of  
9           whom are already engaged in this.

10                   Second, more guidance.

11                   The FAQs that were put out are a useful  
12           first step; and, obviously, there will be more. Those  
13           need to be updated. There will be other issues.

14                   If the Agency issues industry or  
15           individual guidance that is capable of being publicized  
16           or posted, I would suggest you put it on the website.

17                   And, I understand there have been  
18           several comment letters issued to and from the Agency  
19           about that.

20                   Whatever advice you're going to give, if  
21           you could consider preparing a library or an archive of  
22           that to be available on the website, that will help a  
23           number of companies and employers.

24                   Next, there needs to be some real

1 guidance about how to implement these Regs.

2 What, for instance, is meant by "other  
3 portable devices"?

4 Well, we understand PDAs, Blackberries,  
5 Thumb Drives.

6 What about back-up tapes and the process  
7 to back-up the information which you're going to hear a  
8 lot about?

9 Second, what is "reasonably necessary to  
10 accomplish the legitimate purpose?"

11 Those are fairly broad principles; but,  
12 there could be steps or factors at least incorporated  
13 that you could let us know about.

14 Third, with respect to the Vendor issue,  
15 you're going to have a number of questions about what's  
16 the difference between May 1 and January 1 of next year  
17 on the certification?

18 If Vendors are to be compliant by May 1,  
19 why do we need a certification later?

20 If, on the other hand, the real date is  
21 January 1, then, let's say that; but, it's confusing as  
22 to what companies' obligations are and what they need  
23 to secure from Vendors by May 1 of this year.

24 Now, if the response is: this is too

1 complicated; the Agency can't do it; we're not in the  
2 position of giving individual advice, then, there are  
3 ways to get help. There are a number of ways to get  
4 outside assistance for which there is adequate  
5 precedent.

6 A number of Government Agencies have  
7 Advisory Boards, the Feds do it on a number of levels  
8 including the FDA; the State here, the Massachusetts  
9 Commission --

10 [Confusion/Noise]

11 HEARING OFFICER MURRAY: Can you just suspend  
12 a moment?

13 ATTORNEY SCHREIBER: Sure.

14 [Off the Record]

15 HEARING OFFICER MURRAY: I'm sorry, Mark.

16 ATTORNEY SCHREIBER: Sure.

17 So, let me just go back. If the  
18 response is these issues are too complex for the Agency  
19 to address or we cannot give individual advice or it's  
20 too particularized or we need other help, we just can't  
21 do it, there is adequate precedent to obtain help  
22 through Advisory Boards, voluntary or otherwise.

23 The Feds do it, the State has done it.

24 Some years ago, the Mass. Commission

1 Against Discrimination had issues with how do you  
2 handle sexual harassment; and, it was so complex that  
3 folks felt that they needed guidance for that.

4 What the MCAD did, in coordination with  
5 the Massachusetts Bar Association, is they formed a  
6 Joint Committee that was an Advisory Group of the Mass.  
7 Bar that worked with the MCAD for upwards of four (4)  
8 years, which I helped chair; and, ultimately, developed  
9 guidelines that were acceptable both to plaintiffs and  
10 defendants.

11 We know that these Regulations will  
12 carry forward into future years and have significant  
13 import.

14 A similar kind of Advisory Board that  
15 may be useful over the period of -- over a period of  
16 years may be developed by drawing on existing resources  
17 such as the Boston Bar Association Privacy Committee,  
18 the Massachusetts Bar Association or other groups who  
19 have already given you comments.

20 And, I suspect if you ask for a raise of  
21 hands here who'd be willing to be on an Advisory  
22 Committee --

23 [Laughter]

24 -- you'd get a lot of takers.

1 HEARING OFFICER MURRAY: I don't think I'm  
2 going to do that.

3 [Laughter/Comments]

4 ATTORNEY SCHREIBER: But, it is a potential  
5 useful resource.

6 Now, other agencies also say this is  
7 quite difficult to address; but, we heard recently that  
8 the FDA already started putting out guidelines on  
9 identity theft and have step-by-step procedures of how  
10 to address that.

11 This is one of their manuals they gave  
12 us at a Bar Meeting two (2) or three (3) days ago.

13 The Information Commissioner's Office in  
14 the U.K., where they have no Regs on this, managed to  
15 put out detailed guidelines for companies about  
16 Remediation Security Plans. It is very specific and  
17 detailed. It gives lots of useful advice.

18 And, I think one (1) of the suggestions  
19 is, assuming these Regs go into force on May 1, we can  
20 all do a better job of setting out step-by-step  
21 guidelines for companies on how to implement these Regs  
22 and what the factors are; not simply principles in the  
23 FAQs or even in the Model Policy; but, to dive a level  
24 deeper, break it into elements, give guidance,

1 placeholders or otherwise for companies to consider to  
2 actually make a good faith effort to implement the  
3 Regulations.

4 Thank you.

5 HEARING OFFICER MURRAY: Thank you very much.

6 Jon -- Jon Hurst?

7 JON B. HURST: Thank you.

8 ---

9 **Jon B. Hurst**

10 **Retailers Association of Massachusetts**

11 Good afternoon, Mr. Murray.

12 My name is Jon Hurst. I'm President of  
13 the Retailers Association of Massachusetts.

14 I'll be extremely brief because there  
15 are a lot more people that are more -- more  
16 knowledgeable than myself.

17 I have -- I want to present two (2)  
18 written documents for consideration. First, a letter  
19 from 70 organizations, wide variety from Chambers of  
20 Commerce right up to -- to National corporations giving  
21 some pretty explicit information on -- on concerns with  
22 the Regulation and -- and what we would like to see to  
23 work with you going forward to -- to develop a dialogue  
24 and -- and, perhaps, hopefully, a process like we've

1 seen in New Jersey and elsewhere.

2 I, also, have comments directly from the  
3 Retailers Association of Massachusetts.

4 I guess really the bottom line is we're  
5 looking for some time, we're looking for some  
6 reconsideration, we want -- we want to take a look at -  
7 - at what exists and what is becoming -- going to be  
8 existing with -- with Federal Law; and -- and, we need  
9 to do some -- some education.

10 I think the previous speaker was right  
11 on -- on point.

12 I don't think there's been a law -- I  
13 know there hasn't been a law here in Massachusetts as  
14 wide effecting so many different people as -- as --  
15 really since the Healthcare Law -- you know -- when we  
16 passed the Mandatory HealthCare Law -- you know -- that  
17 was -- that effected everybody.

18 This, arguably, effects really anyone  
19 with customers or employees in this State -- you know -  
20 - non-profits, all sorts of organizations.

21 With the HealthCare Law we, literally,  
22 took two and a half (2 1/2) years to -- to implement  
23 that law, to allow for education and compliance.

24 The State, itself, did a lot of work on

1 education and -- and outreach and -- and took a lot of  
2 time to make sure that -- that individuals and  
3 employers alike really fully understood the  
4 ramifications and what the responsibilities of it were.

5 And, we'd like to see a similar time  
6 process and -- and education process on this.

7 Just some brief points: duplication and  
8 conflicts with similar Regulations.

9 I know from our standpoint, from the  
10 Retailers, we have -- all my counterparts in 49 States  
11 right now are wringing their hands trying to get all  
12 their Mom-and-Pop stores and restaurants up to speed to  
13 be -- to be in compliance with the FTC's Red Flag  
14 Rules; and, I -- I respond back to them: well, imagine  
15 putting yourself in my place, I -- I have to try to  
16 educate on not only Red Flag Rules but on a  
17 Massachusetts version which really does -- is not in  
18 sync and -- and may be in conflict.

19 One of our recommendations is -- you  
20 know -- when it comes to something, anything dealing  
21 with Interstate Commerce whether it's products, goods,  
22 services, information -- you know -- ideally, this type  
23 of Regulation is done on the Federal level.

24 In absence of Federal action, States can

1 and should take -- take steps; but, if -- if the Feds  
2 are taking steps, let's make sure that we are not  
3 taking steps that put our people out of sync and at a  
4 disadvantage with -- with others.

5 If we can have a dialog, take a real  
6 close look at what the Red Flag Rules and other rules  
7 that exist with the SEC and with Graham-Leach Blyley  
8 and make sure that we aren't putting our own employers,  
9 our own organizations at -- at a disadvantage with  
10 those and 49 other States. I think that would be  
11 worthwhile.

12 You know, it wasn't that long ago we  
13 passed Do Not Call Lists here in Massachusetts. This  
14 Agency was -- was tasked with implementing that.

15 It was within months that Congress  
16 passed a Federal Law and -- and -- and we did a -- I  
17 believe we did a very good job to make sure that those  
18 laws were really well synced.

19 If you were in compliance with one,  
20 whether you were a Consumer or -- or a Marketer, you  
21 were in compliance with the other.

22 And, we would suggest a similar type of  
23 process on this as well, particularly, given the  
24 reality of what's happening out there in the economy

1 with limited resources and -- and real issues as far as  
2 individuals and employers and just trying to make  
3 payroll, trying to keep the doors open in this economy.

4 Encryption, there are much more  
5 technical people than I to deal with that; but -- you  
6 know -- we believe, particularly from a small business  
7 perspective -- you know -- let's find a reasonable date  
8 to require it; but, really, only require it as you  
9 upgrade systems.

10 If you are a small business and you --  
11 and you -- you're a retailer, you -- you bought new  
12 point-of-sale equipment a couple of years ago and they  
13 can't go back an upgrade it to be in compliance with  
14 this Regulations.

15 Let's allow these businesses really to -  
16 - to be told: this is what you should be doing; next  
17 time you upgrade these systems, next time you replace  
18 these systems, this is what you should be doing on it  
19 from a date going forward as you make those new  
20 investments.

21 A similar type of argument on the third-  
22 party providers, particularly, for a small business  
23 that -- you know -- might not be engaging attorneys and  
24 -- and may not really have a whole lot of ability to --

1 to compromise and write contracts with -- with larger  
2 service providers, third-party entities that they have  
3 to do business with both here in the State and -- and  
4 around the Country and around the World -- you know --  
5 the small businesses are really at a disadvantage  
6 there.

7 And -- And, we don't believe a lot of  
8 these people that we do business with are really going  
9 to agree to -- to drop on a date-certain and  
10 renegotiate a contract or -- or even acknowledge a  
11 Massachusetts Regulation.

12 Let's -- Let's look at -- at requiring  
13 -- you know -- certain --

14 If we're -- If we're going to require  
15 third-party certification and compliance with this  
16 Regulation, let's do it on a going-forward basis as  
17 opposed to: let's drop everything now, throw  
18 everything out and start from scratch.

19 Another -- Another thing that we would  
20 like to raise is -- is applicability to Government  
21 entities.

22 We're not real sure exactly how far this  
23 -- this Regulation really applied to Cities and Towns  
24 and State Government, Federal Government.

1 I think -- I think the reality is that  
2 -- that breaches -- data breaches, about third -- a  
3 third of all data breaches that have occurred have  
4 occurred with Government entities and -- and -- you  
5 know -- if this is a good idea, if it is the right  
6 thing to do, I think what is good for the Goose ought  
7 to be good for the Gander.

8 I think -- you know -- if we aren't  
9 requiring the same to thing to occur with -- with  
10 Government, then, we need to step back and reassess --  
11 you know -- maybe this wasn't such a good idea for our  
12 other employers that are trying to get by in a bad  
13 economy -- you know -- if we can't do this in State  
14 Government and Cities and Towns, why should we make  
15 them do it as well, at least under the same time frame.

16 And -- And, finally, we would -- one  
17 (1) other point we'd like to -- to raise, we are,  
18 certainly, concerned with -- with enforcement of this  
19 Regulation -- you know -- certainly, the -- the time  
20 frame and education is an issue; but, also,  
21 enforcement.

22 We aren't really adverse to having the  
23 Attorney General, certainly, enforce the law; but, we'd  
24 like to see some clarification that it is the Attorney

1 General that -- you know -- solely that enforces this  
2 law. We don't want --

3 We don't believe it was the intent of  
4 the Legislature in any way to allow a private right of  
5 action.

6 For instance, under 93A, we're very  
7 concerned that there could be Bounty Hunter-type of  
8 activity; and, anytime there is a breach here in  
9 Massachusetts, any -- any entity is going to be subject  
10 to demand letters and to be really put at a very large  
11 risk.

12 An explicit statement that this is  
13 solely enforceable by the Attorney General, certainly,  
14 would be -- and not applicable to private right of  
15 action is something we believe should be considered by  
16 this Agency.

17 With that, I will leave you these two  
18 (2) Statements. We -- We hope to work with you on a -  
19 - on a cooperative basis going forward.

20 Thanks very much.

21 HEARING OFFICER MURRAY: Thank you.

22 Tami Salmon?

23 TAMI SALMON: Thank you.

24 ---

1                                   **Tami Salmon**

2                                   **Investment Company Institute**

3                                   My name is Tami Salmon and I'm here  
4 today representing the Mutual Fund Members of the  
5 Investment Company Institute.

6                                   The Institute is the National  
7 Association of the U.S. Mutual Fund Industry.

8                                   Members of the Institute operate in all  
9 50 States, as well as Internationally. They manage  
10 total assets of almost \$10Trillion; and, they serve  
11 almost 93Million shareholders.

12                                   As regards the Commonwealth,  
13 approximately, half of the households here own at least  
14 one (1) Mutual Fund and these shareholders -- Excuse  
15 me. -- account for approximately -- Excuse me. --  
16 \$290Billion in Mutual Fund assets.

17                                   Massachusetts remains the epicenter of  
18 the Mutual Fund industry with Massachusetts investment  
19 companies managing \$2.4Trillion in assets, or 21% of  
20 the total industry assets.

21                                   Importantly, these companies are also  
22 large employers in the Commonwealth, employing over  
23 33,000 persons or, approximately, 20% of the total  
24 employees in the industry.

1                   Many of the Institute's members have  
2                   joined me here today.

3                   It is because of the importance of the  
4                   Commonwealth to the Mutual Fund Industry and the  
5                   industry's concerns with the new data security  
6                   standards that I am here today to discuss the recent  
7                   extension of the compliance date attached to those  
8                   Standards.

9                   As a preliminary matter, I want to  
10                  stress that Mutual Funds have long taken seriously  
11                  their obligation to protect the confidentiality and  
12                  integrity of non-public Consumer information.

13                  This obligation derives not only from  
14                  requirements imposed on us under Federal Law but on  
15                  each fund's interest in protecting its brand image.

16                  Our industry depends on investor trust  
17                  to survive and an important component of that trust is  
18                  protecting the confidentiality, security and integrity  
19                  of shareholders information regardless of where that  
20                  shareholder may reside.

21                  It is for this reason that our members  
22                  have spent tens of millions of dollars on their  
23                  information security systems and why they continue to  
24                  revise them as necessary to ensure they address new and

1 emerging vulnerabilities and threats and that they  
2 adopt new security technologies as appropriate.

3           Notwithstanding that commitment to data  
4 privacy, I am here today both to express the very  
5 serious concerns our members have with the manner and  
6 substance with which the Department of Consumer Affairs  
7 and Business Regulation undertook rulemaking under  
8 Chapter 93H and to comment on the Emergency Rules  
9 issued in December.

10           As you know, my appearance today is not  
11 the first time the Institute has expressed these  
12 concerns.

13           To recap briefly, we first expressed  
14 concerns with the proposed Rules on January 10th, 2008  
15 shortly after their adoption.

16           By letter dated October 8th, 2008, we  
17 expressed our concerns with their extra-territorial  
18 impact and their aggressive compliance date.

19           On November 17th, I met with  
20 representatives of the Department along with 17 Mutual  
21 Fund companies to, again, express our serious concerns  
22 with the overly prescriptive requirements of the Rules  
23 and the aggressive compliance date.

24           On November 19th, I testified before the

1       Legislature's Joint Committee on Consumer Protection  
2       and Professional Licensure regarding our concerns with  
3       the Rules.

4                       On November 26th, at the request of the  
5       Department as a follow-up to our November 17th meeting,  
6       I filed a very lengthy letter with the Department on  
7       behalf of Mutual Funds identifying very specific issues  
8       of concern, including the compliance date, and I sought  
9       clarification of various requirements.

10                      On December 12th, after attending the  
11       conference of the National Association of State  
12       Treasurers where the Standards were discussed in detail  
13       and State Officials expressed serious concerns with the  
14       potential application to such States' activities, I,  
15       again, wrote to the Department.

16                      My last letter to the Department, which  
17       was sent on December 24th, identified each of the  
18       issues from my November 26th letter that the Department  
19       either failed to address or did not address in any  
20       meaningful way.

21                      I provide this history by way of  
22       background regarding our efforts to clearly present to  
23       the Department the serious concerns Mutual Funds have  
24       with the prescriptive, vague and impractical provisions

1 comprising the Standards.

2 Because these efforts, to date, have  
3 been largely unsuccessful in opening a fruitful  
4 dialogue with the Department, I am here, again today,  
5 to reiterate these concerns in the context of the  
6 Emergency Rules.

7 Since today's -- Since today's Hearing  
8 is ostensibly focused on the Department's recent  
9 extension of the compliance date attached to the  
10 Standards, I want to first address this issue.

11 When we met with the Department on  
12 November 17th, we, expressly, asked you how the  
13 Department determined the new compliance date and whom  
14 the Department had consulted to determine its  
15 appropriateness.

16 From the response we received, it  
17 appears that the Department did not consult anyone from  
18 the private sector but determined the new dates were  
19 reasonable on its own.

20 We, respectfully, disagree with your  
21 determination.

22 As presented in our previous  
23 correspondence, we know from our direct experience  
24 implementing Federal Rules that, to the extent they can

1 be implemented, it will take Mutual Funds a minimum of  
2 two (2) years to fully implement the Standards'  
3 requirements.

4 Notwithstanding the absence of it's own  
5 empirical evidence, the Department believes that we can  
6 accomplish this by May 1st for all provisions in the  
7 Standards except encryption of portable devices and  
8 receipt of certifications which it believes we can  
9 comply with by January 1, 2010.

10 The Department has also indicated that  
11 the May 1st compliance date is intended to enable  
12 persons to implement the rules at the same time they  
13 implement the Federal Trade Commission's new "Red Flag  
14 Guidelines" which also have a compliance date of May  
15 1st.

16 This, presumably, reflects the idea that  
17 the two (2) Regulatory Systems are somehow linked and  
18 some efficiency flows from the joint compliance  
19 deadline.

20 We find aligning these two (2)  
21 compliance dates to be most peculiar in light of the  
22 fact that there are no Regulatory similarities between  
23 the Massachusetts Rules and the FTC's Rules.

24 Moreover, many persons subject to

1 Massachusetts' Rules, including many Mutual Fund  
2 companies, are not subject to the FTC's Rules because  
3 they do not permit third-party payments from their  
4 shareholders' accounts.

5 Accordingly, we are at a loss to  
6 understand why the Department deems it appropriate to  
7 link any compliance date for its rules to the FTC's  
8 compliance date.

9 We would add, however, that for those  
10 companies that are subject to the FTC's Rule, the FTC  
11 provided a compliance period of, approximately, 18  
12 months, which is far more time than the Department is  
13 providing to persons to comply with its Rules even  
14 though the FTC's Rules are far less complex than the  
15 Department's Rules.

16 While I know, based upon a Department  
17 letter to me, that the Department believes our members  
18 should have been -- begun implementing the rules as  
19 soon as they were proposed for comment a year ago, such  
20 a response undermines the Public Comment Process.

21 I am not aware of any business that  
22 would expend considerable time, energy and resources on  
23 rule requirements that may or may not be adopted some  
24 day.

1                   Because Mutual Funds' concerns are well  
2 documented through our previous correspondence,  
3 meetings and testimonies, I will not waste your time  
4 today by dwelling on them in any great detail.

5                   I will, however, provide them in hard  
6 copy this afternoon so they become a part of the  
7 permanent record of this Hearing.

8                   Given the nature of this Hearing which  
9 is the question on an appropriate time frame for these  
10 Regulations, I believe it is appropriate to outline for  
11 the record the nature of these concerns and suggest to  
12 you that compliance dates of January -- of May 1st and  
13 January 1st, 2010 are not appropriate because of the  
14 complexity of these issues. These issues include:

15                   First: the fact that the Rules appear  
16 to exceed the Department's Statutory  
17 authority because they are not consistent  
18 with Federal Law as expressly required by  
19 Chapter 93H; nor do the Rules provide  
20 sufficient flexibility based on a person's  
21 size, scope, type of business, amount of  
22 resources, amount of stored data and need for  
23 security and confidentiality of information  
24 as also expressly required by Chapter 93H.

1           Second: the rules will impede Interstate  
2 Commerce because they will preclude the free  
3 movement of information until persons wholly  
4 outside the Commonwealth are willing to  
5 subject themselves to the Commonwealth's  
6 requirements and affirm so in writing.

7           Third: contrary to the Commerce Clause  
8 of the U.S. Constitution, the rules appear to  
9 impermissibly subject other States to the  
10 Commonwealth's Regulatory requirements and  
11 enforcement authority; and, as I have already  
12 personally heard, your sister States are not  
13 willing to submit to your authority and have  
14 no intention of receiving only encrypted  
15 information, modifying their contracts with  
16 our members or others to confirm their  
17 compliance with Massachusetts law or  
18 providing certifications regarding their  
19 compliance as the Standards require them to  
20 do; and

21           Fourth: the Rules are overly  
22 prescriptive and take a one-size-fits-all  
23 approach to data security which makes them  
24 difficult to implement and, ironically, less

1 effective. The difficulty Mutual Funds,  
2 among others, have in implementing the Rules  
3 is exacerbated by the Department's  
4 unwillingness or inability to address very  
5 specific issues raised by the Rules. For  
6 example, who is a third-party vendor?  
7 Without knowing with precision the answer to  
8 this question, persons subject to the Rules  
9 cannot implement them with any degree of  
10 compliance certainty.

11 These comments highlight but a few of  
12 our concerns with the rules and the deficiencies in the  
13 Emergency Amendment to them issued last December.

14 Other concerns we have raised with the  
15 Department that remain unresolved include provisions in  
16 the Rule relating to encryption, the definition of key  
17 undefined terms and the meaning of ambiguous  
18 provisions; each of these have been amply documents in  
19 our correspondence to the Department.

20 In closing, I want to, briefly, raise  
21 two (2) additional issues, one of which I understand  
22 was raised by Senator Morrissey in a recent letter to  
23 Secretary O'Connell and relates to the economic impact  
24 of implementing the Standards.

1 I continue to see quotes in the press  
2 from the Department regarding the de minimis fiscal  
3 impact of the Standards and believe that, if the  
4 Department believes its own quotes, it needs to  
5 undertake a far more rigorous analysis of the fiscal  
6 impact of the Standards than it has done to date.

7 Our members expect to spend millions of  
8 dollars implementing the Rules.

9 Indeed, the testimony presented at the  
10 December Legislative Hearing indicated the serious  
11 concerns businesses, from the smallest companies to the  
12 largest, have with the costs they will incur  
13 implementing the Rules.

14 I look forward to seeing the  
15 Department's response to Senator Morrissey's request  
16 for any serious and credible fiscal analysis that was  
17 conducted in accordance with the Rules' adoption.

18 The final matter I want to raise and  
19 which is most instructive to this Hearing on the  
20 Emergency Rule is what we've already heard previously  
21 about New Jersey's recent experience in adopting rules  
22 to regulate data security and privacy.

23 Like Massachusetts, New Jersey  
24 originally proposed overly prescriptive and unworkable

1 rules that were not consistent with Federal Law, that  
2 did not provide flexibility in their implementation and  
3 that would have been unduly burdensome and costly to  
4 implement.

5 Unlike Massachusetts to date, however,  
6 New Jersey listened to these concerns.

7 The New Jersey Administrators went back  
8 to the drawing board and substantially revised their  
9 Regulations. The revised version has been pre-proposed  
10 for comment by affected persons and the customer and  
11 the public to make sure New Jersey "gets it right"  
12 before even pursuing official adoption.

13 We believe that, by listening to the  
14 regulated community, New Jersey has gotten it right and  
15 we support their revised Regulations.

16 Their pre-proposed rules represent a  
17 well-reasoned, balanced approach to privacy and data  
18 security.

19 It took New Jersey two (2) years to get  
20 their Data Security Regulations right, not including  
21 any implementation time, and to get them pre-proposed  
22 for comment.

23 I, respectfully, submit to you that  
24 Massachusetts simply cannot get it right with what --

1 without first listening to and hearing the concerns of  
2 business and working together with the business  
3 community.

4           Moreover, as indicated by New Jersey's  
5 experience, getting it right involves a deliberative  
6 process where substance takes precedence over haste.

7           In Senator Morrissey's recent letter to  
8 Secretary O'Connell, he suggested that in lieu of  
9 Massachusetts reinventing the wheel, it should be able  
10 to adopt the standards and protections used in other  
11 jurisdictions which -- quote -- ensure a more seamless  
12 transaction data process -- data protection process --

13           We, wholeheartedly, concur with Senator  
14 Morrissey.

15           In light of the near unanimous  
16 opposition to the current form of the Rules, we,  
17 strongly, recommend that the Department heed Senator  
18 Morrissey's advice and consider using New Jersey's  
19 approach as its guide, incorporating a withdrawal of  
20 the current Rules, engaging in a meaningful dialogue  
21 with persons subject to the rules, re-promulgation of  
22 new rules that are both compliant with the express  
23 language of Chapter 93H and consistent with Federal Law  
24 and that appropriately balance the concerns of National

1 and International businesses with the State's interest  
2 in protecting non-public personal information held by  
3 persons conducting business in the State.

4 Additionally, this process should ensure  
5 that, upon adoption, the public is provided ample time  
6 to comply with the Rules.

7 Thank you for your time. My industry  
8 stands ready to work with the Department in adopting  
9 Rules that are effective and achieves the goals the  
10 Legislature intended.

11 HEARING OFFICER MURRAY: Thank you.

12 COURT REPORTER CYR: One (1) moment, please.

13 [Off the Record]

14 Back on the record.

15 HEARING OFFICER MURRAY: Dan Foley?

16 ---

17 **Daniel J. Foley, Jr.**

18 **Massachusetts Association of Insurance Agents**

19 Good afternoon, Mr. Murray.

20 For the record, my name is Dan Foley, F-  
21 O-L-E-Y. I'm Vice President of Government Affairs of  
22 the Massachusetts Association of Independent Insurance  
23 Agents.

24 On behalf of this Association which is a

1 Statewide Trade Association that represents some 1600  
2 independent insurance agencies across the Commonwealth,  
3 I appreciate the opportunity to express our  
4 Association's serious concerns with the provisions of  
5 this Regulation 201 CMR 17.00 and the devastating  
6 financial impact that these Regulation's provisions  
7 will have upon our member agencies.

8 Although the effective date of the  
9 Regulation has been extended to May 1st in some  
10 instances and January 1st, 2010 in other provisions of  
11 the Regulation, this extended time we believe is still  
12 too short for our member agencies to fully comply.

13 We would urge the Patrick Administration  
14 to engage, as has been pointed out by some previous  
15 speakers, in a rigorous stakeholder analysis to provide  
16 an opportunity for comment on the entire set of  
17 Regulations with your Department, with the Attorney  
18 General, with the regulated community as well as  
19 elected officials.

20 Protecting a person's personal  
21 information as defined in the Regulation is very  
22 important and is something the MAIA Members and all  
23 independent agencies take very seriously.

24 However, we believe that there has been

1 a -- that there needs to be a reasonable balance  
2 between protecting a person's identity and the legal  
3 requirements imposed upon the business community in  
4 order to ensure that an individual's personal  
5 information is protected from security breaches.

6 As currently written, we believe these  
7 Regulations go beyond the Legislator's -- Legislature's  
8 intent and mandate specific technologies, creates  
9 redundant and confusing rules and does not hold public  
10 agencies to the standards of the private sector.

11 The standards being imposed upon every  
12 business in Massachusetts that possesses personal  
13 information of a Massachusetts resident will be  
14 especially devastating on our Member Agencies as I have  
15 indicated.

16 We have found that our -- We -- We are  
17 considered truly small business that we represent and  
18 we have found that, in a recent study, that our  
19 Association has conducted to measure the impact of  
20 independent agencies upon the economy in Massachusetts,  
21 the average size agency employs seven (7) employees  
22 with approximately 85% of our Member Agencies having  
23 five (5) or fewer employees.

24 These agencies will not be able to

1 commit the necessary financial resources, both in  
2 personnel and money, to comply with the requirements of  
3 these Regulations by May 1st, 2009.

4 Compliance needs to be based on  
5 resources available and needs to be flexible for small  
6 business as the -- the law that was originally passed  
7 had stated.

8 The current Regulation we believe lacks  
9 flexibility. A one-size-fits-all approach without  
10 regard to the nature of the business and its resources  
11 is inappropriate.

12 The promulgation and implementation of  
13 these specific Regulations are in sharp contrast with  
14 other States, again, as has been point out by other  
15 speakers prior to myself and, especially, other  
16 Massachusetts State Agencies that routinely have  
17 engaged in collaborative discussions with the regulated  
18 Communities.

19 The State of New Jersey, for example,  
20 has recognized that and has held a vigorous stakeholder  
21 analysis; and, we would suggest, as recommended by the  
22 letter that was delivered to Undersecretary Crane and  
23 yourself today, that Massachusetts engage in this type  
24 of process and analysis before full implementation of

1 these Regulations take place.

2 As a member of the Business Coalition  
3 for Data Security, we wholeheartedly certainly support  
4 the recommendations that were put forth in that letter  
5 from the Coalition that makes -- that made relative to  
6 the solutions to the various issues that have been  
7 raised in that letter.

8 I just want to point out, from our  
9 perspective, two (2) or three (3) of the issues that  
10 concern our Member Agencies.

11 Obviously, one (1) major one is the  
12 timing of the Regulations. This is of great concern  
13 and, as I've indicated, we don't feel our members can  
14 fully comply by May 1st and we would urge again the  
15 Administration and your Department to adopt the  
16 suggestions made by the Business Coalition relative to  
17 a phased-in implementation over the Rules over a two  
18 (2) year period.

19 The consistency and contract provisions  
20 and written certification are the other issue that are  
21 of particular concern to agencies.

22 With respect to consistency, the current  
23 Regulations go beyond what the ID Theft Law requires.

24 MAIA members conduct business with

1 clients in other -- and insurance carriers across the  
2 Country; and, it is very important that everyone is  
3 operating on the same page regarding the privacy and  
4 data security laws.

5 The contract and written certification  
6 provisions for third-party service providers we feel  
7 are confusing and unnecessary; and, we, again, would  
8 support the recommendation of the Business Coalition  
9 that contractual language should be used and not  
10 certification.

11 As far as mandatory encryption, the law  
12 doesn't mandate this and its prescriptive nature  
13 negates the reasonableness we believe that is within  
14 the Statute.

15 The inventory requirement under the  
16 Regulation we feel will be very costly and time-  
17 consuming.

18 We support, again, the recommendation  
19 whereby a more meaningful approach would be to  
20 undertake a risk analysis of systems to identify the  
21 potential for loss of such data.

22 Secretary O'Connell was recently quoted  
23 in the Boston Globe where he said that his agency will  
24 spend less energy trying to hire out-of-State

1 businesses to come to Massachusetts and more time  
2 trying to help those already here who -- to help -- to  
3 help them weather the storm in tough times.

4 We believe that, if this is true and  
5 what he says he believes in and given the financial  
6 crisis that we are facing in the Commonwealth, now is  
7 not the time to imposing additional financial burdens  
8 on small business.

9 And, again, we would urge your  
10 Department, the Attorney General, the Regulated  
11 Community and elected Officials to reissue -- to review  
12 and -- and engage in that stakeholder analysis and to  
13 review the entire set Rules with -- and to reissue them  
14 some time in the future with -- with an implementation  
15 update carried out over a two (2) year period.

16 We are willing as an Association to work  
17 with your Department and others engaged in this  
18 process.

19 I thank you for your consideration in  
20 allowing me the opportunity to share our concerns with  
21 you and look forward to working with you in the future.

22 HEARING OFFICER MURRAY: Thanks, Dan.

23 Brad MacDougall?

24 Hi, Brad.

1 BRADLEY A. MacDOUGALL: I'll stand and be  
2 brief.

3 ---

4 **Bradley A. MacDougall**

5 **Associated Industries of Massachusetts**

6 My name is Brad MacDougall. I represent  
7 Associated Industries of Massachusetts. We have 6500  
8 members representing every sector of the economy.

9 And, clearly -- And, some of our  
10 members communicated directly with the Department and  
11 several of the members are here today and -- and we  
12 would appreciate that those folks are actually going to  
13 testify and would urge the Department to listen to  
14 their specific concerns.

15 We agree, from AIM's position, clearly,  
16 that this data protection is a good public policy.

17 The question we have before us today,  
18 though, is how do we get there; and, the how includes  
19 the time and the what included in these Regulations.

20 So, the context and how we do it are  
21 both inexplicably connected and we would urge the  
22 Department to listen to those here present today to the  
23 Business Coalition letter that was submitted to the  
24 Department, to AIM's testimony that is provided to you

1 today, as well as any information that is given further  
2 today.

3           Clearly, there are several issues that  
4 are outstanding and need to be addressed because our  
5 economy truly does depend on it.

6           And, you, clearly, do have a great group  
7 of people here in the room that are willing, ready and  
8 -- to serve as an Advisory Group as someone had  
9 mentioned before.

10           And, we appreciate this opportunity and  
11 thank you and urge you to consider significantly the --  
12 the detrimental impacts of these Regulations on our  
13 economy in going forward.

14           I thank you for this opportunity and  
15 thank you for -- the Administration for the initial  
16 delay and we look forward to continue in working with  
17 the Department to effectuate a more perfect set of  
18 public policy measures to protect data.

19           HEARING OFFICER MURRAY: Thank you.

20                   Andrea Cramer?

21                           ---

22                           Attorney Andrea Cramer

23                           HIRSCH ROBERTS WEINSTEIN -- AIM

24                           Good afternoon!

1 My name is Andrea Cramer and I'm an  
2 attorney in the Litigation and Labor and Employment law  
3 firm of Hirsch Roberts Weinstein; and, we are members  
4 of AIM. We are one (1) the people here testifying  
5 related to AIM.

6 Many of my firm's clients are small  
7 business, including non-profit Community Service  
8 organizations, family and privately owned business with  
9 fewer than 50 employees and Social Service Agencies.

10 My law firm, itself, is a small  
11 business.

12 My experience with these clients and  
13 with my law firm in trying to implement these  
14 Regulations suggest that among the many problems that  
15 you've heard here today, one (1) of them is that they  
16 don't distinguish between customer information and  
17 employee information or between small employers and  
18 large businesses.

19 Well, any security breach that leads to  
20 wrongful actions has a detrimental effect on both the  
21 individual and the third-parties none of us here are  
22 minimizing. Not all breaches lead to the same degree  
23 of harm and not all businesses pose the same level of  
24 risks.

1                   Indeed, the Regulation -- the Report  
2                   that was issued last Fall on the notifications of data  
3                   breaches reported that during the first ten (10) months  
4                   of the new Law only four (4) of the 318 breaches were  
5                   in not-for-profit businesses.

6                   About 80% of the breaches were in the  
7                   Financial Service Sector alone; not in small companies  
8                   like my clients that provide Civil Engineering or  
9                   Computer Services of Scientific Research.

10                  And, where the small businesses and not-  
11                  for-profit companies had breaches, the numbers of  
12                  individuals affected was disproportionately small.

13                  The Report stated that the vast bulk of  
14                  the breaches involving more than 500 Massachusetts  
15                  residents were in the Financial Services industry.

16                  I'm here today on behalf of my clients  
17                  but not on behalf of any single client to say that the  
18                  cost benefit of influencing the entire Regulatory  
19                  scheme is skewed and out of balance for small employers  
20                  who do not store or maintain personal information on  
21                  customers.

22                  Parts of these Regulations will require  
23                  significant operational changes for these business and  
24                  will also impose not inconsequential costs, something

1 that cannot be overlooked in this economy as these  
2 types of businesses are struggling to stay open and  
3 limit layoffs.

4 In this regard, it is important to know  
5 that the estimate of a \$10,000.00 cost of compliance  
6 and maintenance for the first year that the Office  
7 issued is far too low. Some have calculated that  
8 amount to be as high as \$50,000.00; that often is more  
9 than one (1) employee's salary and benefits.

10 Rather than going through all the  
11 details, I'm going to use my time here today to just  
12 give you three (3) examples of how the Regulations in  
13 their current form affects small businesses that do not  
14 have customer information.

15 First, the Regulations require every  
16 comprehensive information security program to include  
17 Security Policies for employees about how to keep,  
18 access and transport records containing personal  
19 information outside the business premises. This takes  
20 time and money.

21 As a point of contrast, even the  
22 Commonwealth's Sexual Harassment Laws do not require  
23 every employer to have a written policy.

24 Indeed, though sexual harassment is a

1 serious problem, even if you work in a small company,  
2 the law does not apply to employers with fewer than six  
3 (6) employees.

4 That's not to say that most employers do  
5 not eventually have written policies as you would want  
6 them to have; but, requiring every single one of them  
7 to do so by May 2009 is grossly over-broad.

8 Beyond the monetary cost, there lost --  
9 there is lost productivity as someone in a small  
10 business has to create and implement the policy.

11 Second, the Regulations require  
12 restrictions on physical access not just to electronic  
13 documents; but, also, to paper records.

14 The analysis the office did on the cost  
15 seems to assume that a ten (10) person company has  
16 lockable file cabinets and -- and locks on all the  
17 doors and that the additional requirements are just  
18 some additional oversight. This is not necessarily  
19 true.

20 As my own law firm is learning, the  
21 Regulations may require purchasing new file cabinets  
22 with locks at a cost of hundreds or thousands of  
23 dollars.

24 We're also trying to figure out whether

1 the Human Resource people in our -- of our clients have  
2 to lock their doors every time they leave their office  
3 if they're working on paper -- with paper documents;  
4 and, whether law firms and consulting firms and things  
5 -- and other firms of that type that incidently have  
6 personal information deep within reams of other  
7 information must implement expensive and time consuming  
8 restrictions just because of the occasional piece of  
9 personal information they have.

10 Just to give you an example of what that  
11 is, in the context of litigation in employment or  
12 business disputes, we often have, as part of the  
13 Discovery process, an employee's Social Security number  
14 or a business' or employee's tax return. Those are  
15 usually part of very large files. These Regulations  
16 seemingly require us to secure -- either to secure the  
17 entire file or to somehow segregate out that single  
18 piece of information within thousands of pages of  
19 documents.

20 Again, this is a monetary and efficiency  
21 cost to companies already struggling in a down economy.

22 Third, the Regulations require that, by  
23 May 1st, every company must contractually require all  
24 30 -- third-party service providers to maintain the

1 mandated safeguards.

2           You've heard other comments on this and  
3 we don't disagree with those; but, specifically, in the  
4 context of the small businesses we represent, they may  
5 not be able to renegotiate contracts that are not  
6 coming due before May 1st; and, in fact, many of their  
7 contracts are with small business who may not be able  
8 to ensure compliance.

9           Again, there is an administrative and  
10 financial cost with the compliance if it's doable at  
11 all.

12           Looking at this practically, the risk  
13 posed from the random piece of personal information  
14 that may be accidentally disclosed in a small business  
15 about customer information is not really much different  
16 from the risk posed by leaving a credit card receipt on  
17 a table in a restaurant or having your mail intercepted  
18 or someone looking over your shoulder in the check-out  
19 line at a department store.

20           Sure, we'd like to stop all fraud and  
21 wrongful actions that can occur from identity theft;  
22 but, as a society, we realize that the cost of  
23 eliminating every one of those risks does not out-weigh  
24 the benefits. The Regulations, as written, do not take

1 that into account.

2 The Regulations say that they -- the  
3 requirements for compliance are not one-size-fits-all  
4 and that factors such as size, scope and type of  
5 business will be taken into account; but, they give no  
6 real guidance on that.

7 And, the reality is that, without the  
8 clearer guidance and explicit exceptions for small  
9 businesses, many business, including many of my clients  
10 whose compliance with all Regulatory schemes is  
11 important to them, will over-protect and incur expense  
12 and time to do that so -- rather than litigate non-  
13 compliance and also risk being fined and held civilly  
14 liable later.

15 As Mr. MacDougall said --

16 HEARING OFFICER MURRAY: Could you just  
17 suspend for a minute?

18 Would everyone, please, take care of  
19 their cellphones so that we're not interrupted.

20 ATTORNEY ANDREA CRAMER: Thank you.

21 HEARING OFFICER MURRAY: My apologies.

22 ATTORNEY ANDREA CRAMER: Not at all.

23 As Mr. MacDougall said, Massachusetts is  
24 to be commended for going beyond the mere reporting

1 requirements that many States have implemented in  
2 seeking to prevent breaches; but, is now -- as now  
3 written, the Regulations are akin to clear-cutting all  
4 the trees in Worcester to eradicate the Longhorn  
5 Beetles instead of just getting rid of the obviously  
6 infested trees.

7           Though the consequences are not the  
8 same, small businesses that do not have customer  
9 information are being unnecessarily harmed in an effort  
10 to eradicate all identity theft which could never  
11 happen anyway.

12           For these reasons, on behalf of the  
13 small businesses I represent, I urge -- we urge the  
14 Office to reconsider the applicability of the  
15 Regulations to employee information in small  
16 businesses; or, at least, to extend the deadlines for  
17 compliance for businesses of 50 or fewer employees  
18 which do not store or maintain customer information, at  
19 least, for another year if not longer as many of the  
20 other people here have testified.

21           During that time, much will be learned  
22 about -- from the compliance attempts at other -- at  
23 larger places of employment and that information can be  
24 used to reevaluate the Regulations as a whole and,

1 particularly, their applicability to small businesses  
2 and non-profits that do not have personal information  
3 of customers.

4 Thank you.

5 HEARING OFFICER MURRAY: Thank you.

6 Michael Ripple?

7 MICHAEL RIPPLE: Good afternoon! Thank you  
8 for this opportunity.

9 HEARING OFFICER MURRAY: Thank you for  
10 coming.

11

---

12

**Michael Ripple**

13

**Massachusetts Council of Human Service Providers**

14

MICHAEL RIPPLE: My name is Michael Ripple,

15

R-I-P-P-L-E.

16

17

18

19

20

21

I'm the Director of Operations for the  
Massachusetts Council of Human Service Providers. We  
are a Trade Association representing non-profit  
organizations of mostly 501-C(3)s independent of the  
State; but, they receive a great deal of money from the  
State.

22

23

24

And, they do this through contracts and  
receive \$2.7 Billion from the Commonwealth which is,  
approximately, ten (10%) percent of the State Budget.

1                   The services they provide are for the  
2 Homeless, people who are victims of domestic violence,  
3 adoption services, Substance Abuse Services, people  
4 with all ranges of mental and physical abilities --  
5 disabilities -- Excuse me. -- and operate through  
6 5500 sites across the Commonwealth.

7                   And, this -- this Sector is today asking  
8 to be exempt from these Regulations.

9                   We're -- We're doing this for two (2)  
10 reasons.

11                   Primarily, we are an extension of the  
12 State and, by extension, the Federal Government and we  
13 comply with all of their Regulations.

14                   Confidentiality of the individuals that  
15 our members serve, Community-based services serve is  
16 paramount to us and we comply with all the current  
17 Regulations.

18                   We fill Legislative mandates. What we  
19 do in our compliance is defined in contracts.

20                   We have no commercial activity and the  
21 exchange of all information is with the State, nowhere  
22 else.

23                   Our second reason is our sector has been  
24 level-funded since 1988.

1                   We haven't had one (1) penny  
2                   appropriated by the Legislature to increase our  
3                   operating funds.

4                   All expenditures are prescribed in  
5                   contracts to meet State Licensing Standards and  
6                   Building Codes, whatever.

7                   And, as a result of this 20 years of  
8                   level-funding, our budgets are absolutely in-elastic  
9                   and there are -- there are no mechanisms to get money  
10                  to pay for these expensive Regulations; and, there's no  
11                  mechanism within the State to provide it.

12                  And, particularly in this economy, this  
13                  situation is absolutely compounded and the fiscal  
14                  plight of our sector has been well documented by the  
15                  Executive Office of Health and Human Services.

16                  So, basically, the funds don't exist for  
17                  us to comply with this.

18                  And, it's -- it's -- it's hard enough to  
19                  come around to find money to provide the essential  
20                  services to one (1) in ten (10) residents of the  
21                  Commonwealth that are most vulnerable who require them.

22                  And, we, certainly, just don't have the  
23                  funds to comply with these Regulations and seek  
24                  exemption from them.

1 Thank you.

2 HEARING OFFICER MURRAY: Thank you.

3 Jack Daniel?

4 COURT REPORTER CYR: Somebody -- Excuse me.

5 [Door to Hall Closed]

6 Thank you.

7 HEARING OFFICER MURRAY: Mr. Daniel?

8 JACK DANIEL: Thank you.

9 ---

10 **Jack Daniel**

11 **Internet & Network Security Vendor**

12 My name is Jack Daniel. It really is.

13 [Laughter]

14 The last name is D-A-N-I-E-L. I'm here on my own.

15 I do work for a company that actually  
16 might profit from some of this, Internet Security and  
17 Network Security equipment vendor.

18 But, I'm here because several people  
19 have asked me to look into 201 CMR 17.00. I have  
20 spoken to a couple of groups about it.

21 And, I'd like to share some observations  
22 which I think lead to at least asking for a delay of  
23 implementation and review of some things.

24 I'd like to start out by saying, at the

1 first reading of the Law, it's fairly concise, it seems  
2 flexible.

3 When you read down the bullet points, to  
4 someone who is an Information Security professional,  
5 it's a list of common sense Regulations, guidelines,  
6 things that are very hard to argue with at face value.

7 But, one (1) of the problems that we  
8 face is that there is, first of all, a lack of common  
9 sense in the World and attempts at legislating common  
10 sense also tend to run into -- run into issues -- you  
11 know -- a lot of push back.

12 And, when you dig a little bit deeper, a  
13 lot of these, really, are not as simple as they look at  
14 face value.

15 A couple of things I'll say may not sit  
16 well with some of the business folk.

17 One (1) of the things I'll say is I  
18 don't have a problem as a Citizen of the Commonwealth  
19 or as a technology professional with the State taking a  
20 leadership role in an issue which has caused an  
21 enormous amount of grief and financial loss for people  
22 throughout the World and in the Commonwealth.

23 We have the three (3) letter company  
24 down the road and -- and we can do more, especially in

1 my industry.

2 So, I don't have a problem with leading;  
3 but, we have to lead well I think is what I would  
4 request. I'd like to go over a couple of things very  
5 quickly.

6 I work with a lot of small companies.  
7 The awareness issue is substantial. Small companies  
8 are simply unaware of this that's all. Other people  
9 have said it more eloquently.

10 The encryption issues, I think, again,  
11 the small business have a large burden with encryption.

12 As an technology professional, I can  
13 solve any of these encryption issues for myself in a  
14 matter of seconds with free stuff; but, if I had --

15 I have some consulting customers who are  
16 in the 15 to 150 employee range and they have more  
17 machines that need encryption than are simply done by  
18 two (2) or three (3) people getting together and coming  
19 up with a plan; but, not enough to write a check to one  
20 (1) of the companies that -- there's several here in  
21 Massachusetts who will sell you a solution. It's a  
22 large check to buy that.

23 You need to be 250 or more employees;  
24 and, even at that point in time, it's a lot of money.

1           There are just a lot of small and medium  
2 sized companies for whom encryption, even though I feel  
3 is a key component of this, I think that getting it  
4 right is going to be difficult for a lot of small and  
5 mid-sized companies.

6           I do think that a lot of the technology  
7 for encryption is mature, stable, reliable.

8           I think the problems come in ease of  
9 deployment and ease of expense particularly for the  
10 smaller enterprises.

11           It's been touched on before, the  
12 penalties are somewhat nebulous. There are no specific  
13 penalties.

14           The only document that I found, perhaps,  
15 I missed it, 93I does have specifics for destruction  
16 and disposal and that's solid; but, it is sort of  
17 vague.

18           We -- We have -- As a society, we have  
19 an idea of what -- what the penalty is for traveling 90  
20 miles an hour down the Mass. Pike; we have -- we have  
21 an idea what the penalty is for Tax Fraud; we have an  
22 idea -- This is very vague and, while it does sort of  
23 undermine the law, there is a risk analysis that people  
24 make.

1                   If the penalty for getting caught going  
2                   90 miles an hour on the Mass. Pike were \$3.00, more  
3                   people would speed; but, it is just a big question mark  
4                   for a lot of people.

5                   Also, one (1) of the things that I'll  
6                   say that also will somewhat upset some of the people in  
7                   the industry, as someone who lives and breathes  
8                   information security, inventory of information is a  
9                   fundamental tenant of information security; but, it is  
10                  not easy and it is not inexpensive.

11                  So, what I would propose for that is  
12                  additional time to do it well.

13                  I -- I am very much in favor of the  
14                  object of this and most of the things that I see here  
15                  are doable in time.

16                  But, I feel there'll be either a rush  
17                  and do them poorly to fill the check-box to get into  
18                  the situation the industries are in, PCI, the whole  
19                  litany of compliance issues where it's boiled down to a  
20                  check-box whether or not it actually moves us forward.

21                  And, the amount of effort that you've  
22                  put in, the Commonwealth has put in, the Legislature  
23                  has put in to make this happen, I think we should do  
24                  this right; and, as I said, I don't have a problem

1 leading, I just think we should lead in the right  
2 direction.

3 And so, yeah, that's about it.

4 I will throw one (1) idea out that is  
5 not really a suggestion for legislation; but, to take  
6 it in a different direction.

7 Sometimes, people transfer risk; it's  
8 called insurance. There's a lot of that in this State.

9 An alternative to this is to simply say  
10 that businesses are liable for a certain amount of  
11 money for losses in data. If they acquire insurance,  
12 if they secure themselves, it's risk transference; and,  
13 what'll happen is it will be just like fire insurance  
14 for your business.

15 You go out and you buy insurance, the  
16 Insurance Agent is probably going to come in and tell  
17 you to do everything that matches the checklist you  
18 have in -- in front of you; but, it's -- it's done in  
19 the marketplace.

20 And, with that, I'll let the next folks  
21 go on; but, I appreciate the opportunity to speak.

22 Thank you very much.

23 HEARING OFFICER MURRAY: Thank you.

24 Mary Ann?

1 MARY ANN CLANCY: Thank you, Mr. Murray.

2 HEARING OFFICER MURRAY: Why don't you have a  
3 seat.

4 MARY ANN CLANCY: I'll be quick. It's okay.

5 HEARING OFFICER MURRAY: It's all right.  
6 Have a seat.

7

---

8 **Mary Ann Clancy**

9 **Massachusetts Credit Union League, Inc.**

10 MARY ANN CLANCY: On behalf of -- My last --  
11 My name is, for the record, Mary Ann  
12 Clancy, C-L-A-N-C-Y.

13 I serve the Massachusetts Credit Union  
14 League, a Trade Association for Credit Unions in the  
15 Commonwealth.

16 We serve about 2.4Million members; so,  
17 about one (1) in three (3) Consumers are members of a  
18 Credit Union which we have a relationship with.

19 We appreciate the hard work, certainly,  
20 of yourself, Mr. Murray, members of your Staff,  
21 Director Crane, Secretary O'Connell and everyone in  
22 between.

23 We, certainly, support the efforts  
24 you've done before. They are commendable bringing a

1 case of first impression with these Regulations forward  
2 are all things that we think are very important.

3 We, also, were very appreciative of the  
4 extension that you've already done with respect to the  
5 Regulations.

6 The issue of the protection of data for  
7 Consumers for us is absolutely paramount.

8 All -- All you have to do is look to  
9 the fact that Credit Unions are amongst the first  
10 responders to reissue plastic cards in instances of  
11 fraud or data compromises up until now at our own  
12 expense. It's part of our own business decision as a  
13 way of sticking to our mission in serving members.

14 We understand it. We get it. And, we  
15 think your efforts are very, very commendable.

16 I'm here today for the purpose of the  
17 Hearing which is really related to the extension; and,  
18 we would ask for consideration, perhaps, through the  
19 Calendar Year 2010.

20 Our reasons for that are really tied to  
21 a more specific, substantive provision of the  
22 Regulation which we brought forward in the Hearing last  
23 January before you; and, that is the issue of the  
24 compliance with Federal provisions.

1                   When we worked in order to get to the  
2 Regulation when the Statute was done, Chairman Rogers  
3 reached out to us, someone who was very intricately  
4 familiar with Credit Unions -- We have over 50 Credit  
5 Unions that are under \$5Million in assets with one (1)  
6 or two (2) employees. -- and, he said explain to me  
7 how this works, explain to me what the concerns are.

8                   We reiterated that, with GLB, we were  
9 under that and our Federal Regulator who covers all  
10 Credit Unions had a series of Regs since 2001 that were  
11 in it. It was our understanding that Section 5 of the  
12 Law was intended to actually look at that and to have a  
13 safe harbor in place.

14                   Much like other parts of the rule, we  
15 also had, we thought encryption was an incentive; but,  
16 I'm not here to go into all of that and our -- our  
17 statement, certainly, addresses some of that.

18                   We share that with you somewhat  
19 anecdotally; but, it is related to the reason why, if  
20 the Regs stay as they are, that we would have concerns  
21 and be looking for an extension -- a further extension  
22 of the compliance date.

23                   With that, unless you have any  
24 questions, again, we, respectfully, offer the comments,

1 offer the concerns and would be happy to work with you  
2 as you go forward.

3 HEARING OFFICER MURRAY: Thank you.

4 Tim Sweeney?

5 ---

6 **Timothy Sweeney**

7 **Greater Boston Chamber of Commerce**

8 TIMOTHY SWEENEY: Good afternoon. My name is  
9 Tim Sweeney, S-W-E-E-N-E-Y; and, I'm Director of Public  
10 Policy with the Greater Boston Chamber of Commerce.

11 The Chamber would like to submit  
12 testimony on behalf of its 1700 Members, all of which  
13 will be impacted by these Regulations.

14 And, I'd like to -- to thank -- thank  
15 you, Mr. Murray, Undersecretary Crane, the  
16 Administration and the entire team both for the  
17 opportunity to testify and also for your willingness to  
18 engage the Chamber and its Members on this important  
19 issue; so, we thank you for that.

20 We'd also like to acknowledge and thank  
21 the decision by the OCABR last Fall to delay the  
22 effective dates. We felt that such delay was  
23 absolutely essential for companies seeking to be  
24 compliant with these new requirements.

1           Ensuring data privacy is a goal that we  
2 share and we believe it can be addressed through --  
3 through regulation without significantly impacting  
4 jobs, investments or overall competitiveness.

5           The implementation delays were a  
6 positive step in that direction; however, we think that  
7 there are also requirements within the -- the  
8 Regulation that merit further discussion and  
9 consideration.

10           First category is definitions and, more  
11 specifically, personal information.

12           While it's not, specifically, cited in  
13 the Regulation, companies have told us that they are  
14 concerned that customer account numbers such as those  
15 used by Utilities and other industries would be treated  
16 in the same way that a Social Security number or  
17 financial account number is treated in the Regulation.

18           Unlike those numbers, customer account  
19 numbers can't be used to withdraw funds or establish  
20 another person's identity; so, we would recommend  
21 revising the Regulation to remove this uncertainty and  
22 to ensure that -- that such customer account numbers  
23 are not subject to the Regulation.

24           Second category is encryption and,

1 actually, the retroactivity issue.

2 We recommend that encryption be required  
3 only a going-forward basis for new investment, upgrade  
4 or equipment purchase after the effective date of the  
5 Regulation.

6 Adding encryption capabilities  
7 retroactively to systems that are already in place  
8 could be very difficult and costly.

9 And, secondly, flexibility in  
10 technology, prescribing specific encryption  
11 technologies would prevent companies from employing  
12 cutting edge solutions in this field -- in this rapidly  
13 evolving field.

14 And, it is our understanding that the  
15 Agency didn't intent to be overly prescriptive in terms  
16 of which technologies are used as long as the  
17 encryption is -- is achieved.

18 We think such latitude would enable next  
19 general technologies to be employed; and, we agree with  
20 this thoughtful approach and ask that it be codified in  
21 the final Regulation.

22 Next is inventory; and, this has been  
23 discussed several times today; but, this is a process  
24 that could take months or years to complete for many

1 companies and would involve not only substantial up-  
2 front costs; but, also, on-going cost due to the  
3 evolving -- evolving nature of data storage systems.

4 We ask that the Agency consider a more  
5 risk-based approach to compliance allowing companies to  
6 implement plans based on the data they keep and the  
7 potential loss for such data focusing privacy resources  
8 where they're needed most.

9 Next category is third-party vendor --  
10 vendor certification. While dealing with vendors,  
11 companies often insist on and negotiate contractual  
12 language guarantying safety and security of their  
13 customer's personal information.

14 Best practices such as this are  
15 essential to securing a company's reputation, long term  
16 viability and commitments to -- commitment to its  
17 customers.

18 Many of our larger companies have  
19 hundreds if not over a thousand vendor contracts  
20 currently in place and the prospect of having to reopen  
21 or renegotiate such existing contracts to satisfy this  
22 requirement would prove immensely costly, time  
23 consuming and, in some cases, unworkable, especially,  
24 if vendors are located outside of Massachusetts, if

1 they're the only vendor -- perhaps, the only vendor in  
2 this market offering a particular service or product or  
3 if they are simply unwilling to certify compliance to a  
4 requirement while they are under an existing contract.

5 As such, we would ask consideration for  
6 a removal of the third-party vendor certification  
7 requirement.

8 If the removal of this requirement can  
9 not be accommodated in the Regulations, we ask that the  
10 following revisions be considered in order to make this  
11 provision more workable:

12 One, to eliminate the  
13 retroactivity of vendor  
14 certification requiring only  
15 certifications as part of a new  
16 contract that would be inked after  
17 the effective date of the -- of  
18 this provision.

19 Requiring certification on a  
20 going-forward basis is consistent  
21 with the allowances made for Public  
22 Agencies in Executive Order 504;  
23 and, if Public Agencies are allowed  
24 to certify vendors on a -- on a

1 going-forward basis, we feel that  
2 companies should also be governed  
3 by the same principle.

4 And, also, we ask for  
5 consideration for inserting  
6 language that would require a  
7 company to only obtain compliance  
8 certification from vendors that  
9 they directly contract with.

10 It is our understanding that  
11 this was the Agency's intent;  
12 however, codifying language in this  
13 Regulation would require certain  
14 companies engaging in multi-party  
15 transactions such as routinely  
16 occurs in Financial Services that  
17 they need not certify each vendor  
18 that their primary vendor utilizes  
19 in order to execute a transaction.

20 Next category is personal information  
21 collection.

22 The collection and retention of personal  
23 customer information has been a standard business  
24 practice for companies of all size and industry and if

1 we are to impose overly restrictive limits on both the  
2 amount of information collected and the time it can be  
3 retained, we could end up disrupting longstanding  
4 operational processes while limiting marketing,  
5 advertising and customer service options and placing  
6 our companies at a distinct competitive disadvantage.

7 We ask for consideration that this  
8 clause be removed from the Regulation.

9 And, lastly, the last category is the  
10 compliance checklist -- the Small Business Compliance  
11 Checklist.

12 We -- We, really, appreciate the  
13 Agency's responsiveness to address the on-going  
14 concerns that small businesses and individuals have  
15 with -- in their efforts to come into compliance with  
16 the Regulation; yet, we believe that implementing many  
17 of the items on this checklist would prove unworkable  
18 or cost and resource prohibitive to small businesses.

19 Given the hurdles that small businesses  
20 face these days with our -- with our economic  
21 situation, we believe the checklist might be better  
22 presented as a set of possible options for small  
23 businesses or individuals to consider rather than a set  
24 of items that -- quote -- require attention in order

1 for a plan to be compliant.

2           Such a revision would reflect the intent  
3 of the Regulation and its allowance for compliance  
4 scaleability -- [Phonetic] -- based on size, scope,  
5 type of business, available resource and need for data  
6 security and confidentiality.

7           In closing, the Regulations will impact  
8 companies of all sizes industry at a time of widespread  
9 budgetary restraint and accelerating revenue and job  
10 loss. The cost and operation burden of any new  
11 Regulation must be viewed in part through this lens.

12           In addition, the lack of awareness  
13 persists among many employers and uncertainties about  
14 compliance and impacts remain among those employers who  
15 are aware of the new requirements.

16           As such, the Chamber looks forward to  
17 continuing this -- this discussion in the days ahead  
18 and working toward the implementation of a Data Privacy  
19 Regulation that furthers our commonly shared goals of  
20 protecting personal information and growing the  
21 economy.

22           Again, Mr. Murray, we thank you for your  
23 time. We thank the Agency for its efforts in this  
24 regard and for the opportunity to testify.

1                   And, I, also, have more descriptive  
2 language changes -- [Inaudible] --

3                   HEARING OFFICER MURRAY: Thank you.

4                   Bob McCarin?

5                   ROBERT McCARIN: Good afternoon, Mr. Murray.

6                   HEARING OFFICER MURRAY: Good afternoon.

7                   ---

8                   **Robert McCarin**

9                   **AICUM**

10                  ROBERT McCARIN: My name is Robert McCarin.  
11 I am the Vice President for Government Relations for  
12 AICUM which is the Association of Independent Colleges  
13 and Universities in Massachusetts.

14                  AICUM represents the interests of 59  
15 independent Colleges and Universities throughout  
16 Massachusetts. The -- These institutions --  
17 250,000 students attend these  
18 institutions and, approximately, 100,000 Massachusetts  
19 residents are employed at these institutions.

20                  I want to thank you for the opportunity  
21 this afternoon to comment on the Amended Regulations.

22                  The Colleges and Universities support  
23 the principles and goals and we would applaud Governor  
24 Patrick and Undersecretary Crane for their effort.

1           The Colleges are already taking  
2 affirmative steps to protect the personal information  
3 of their students, employees and alumni; however,  
4 echoing a lot of the comments you've already heard this  
5 afternoon, the Regulations and, particularly, the  
6 current deadlines under the Regulations are virtually  
7 impossible for the Colleges and Universities to meet.

8           I'd like to, briefly, highlight four (4)  
9 areas of concern that all pertain to the timeline that  
10 they are currently operating under.

11           The first is cost. The Regulations,  
12 essentially, impose a substantial unfunded mandate on  
13 Colleges and Universities. These institution will  
14 incur significant incremental costs as a result of  
15 having to purchase new software and technology.

16           They'll also required to reallocate  
17 existing Staff in which scarce resources to comply with  
18 the Regulations.

19           This unfunded mandate comes at a  
20 particularly difficult time for all business sectors,  
21 including Colleges and Universities.

22           The on-going financial crisis has  
23 significantly reduced the value of endowments,  
24 restricted other revenue streams and required schools

1 to direct scarce resources towards financial aid to  
2 help student continue to continue their education.

3 Many -- Many institutions have  
4 instituted budgetary and hiring freezes.

5 And, add to this the additional  
6 requirements that schools are trying to deal with right  
7 now, including Reauthorization of the Higher Education  
8 Act, changes to FURPUR -- [Phonetic] -- and the FTC Red  
9 Flag Rules. Colleges and Universities are expending  
10 resources to try to comply with these and the  
11 additional burden imposed by these Regulations require  
12 that additional time be given for further study of the  
13 Regulations and further -- and compliance.

14 The second category of concern is third-  
15 party verification.

16 The third-party certification provisions  
17 included in the Regulations are unduly complex  
18 requiring extensive resources and due diligence to  
19 certify compliance.

20 Most Colleges and Universities have  
21 hundreds, perhaps, thousands of contracts with outside  
22 vendors, a significant portion of which relate to data  
23 and documents that contain personal information.

24 Many of these contracts have been in

1 place for years and already contain provisions designed  
2 to protect personal information.

3 To the extent that these pre-existing  
4 contracts do not meet the requirements of the  
5 Regulations, they will have to be renegotiated and this  
6 would take time -- a considerable amount of time.

7 Obtaining assurances from third-party  
8 vendors is a massive undertaking.

9 Doing so before January 1, 2010 will be  
10 virtually impossible for the member institutions of  
11 AICUM, particularly, for smaller institutions with lean  
12 and already over-burdened IT Staff.

13 It makes little sense to enact  
14 Regulations with the knowledge that such a wide range  
15 of institutions and business will have an extremely  
16 difficult time meeting them.

17 The third area that is of concern to  
18 AICUM is the inventory requirement. Colleges and  
19 Universities have a -- a huge volume of records that  
20 conceivably come within the scope of these Regulations  
21 and this information is widely distributed across  
22 several departments on campus.

23 Colleges and Universities are already  
24 striving to protect the personal information of

1 students, employees, donors and alumni.

2 For example, virtually no school uses a  
3 student's Social Security number as a student ID  
4 anymore.

5 The huge inventory undertaking to  
6 coordinate the records and what steps must be taken to  
7 comply with these Regulations is going to take a  
8 significant amount of time.

9 I know some schools that have convened a  
10 Working Group. The Group is trying to develop a formal  
11 project; they're identifying key goals; they're trying  
12 to address these goals sequentially and -- and develop  
13 procedures and refine those procedures.

14 Again, they've started to do this; but,  
15 it is just going to take a lot more time given the  
16 volume of records that schools have on hand now and are  
17 required to keep for students that attended in the  
18 past.

19 We would suggest that getting it right  
20 is more important than trying to meet what seems to be  
21 an arbitrary deadline.

22 The fourth area that is of concern to  
23 the schools is the encryption requirement.

24 This is a sweeping mandate that goes

1 beyond the original Legislative intent.

2 It will require an investment in  
3 software and hardware that is complex, expensive and  
4 time-consuming. Particularly onerous --

5 This is particularly onerous for schools  
6 with lean and an over-burdened Staff. The job of  
7 evaluating, implementing and supporting encryption will  
8 fall exclusively on the IT Staff at these school.

9 I think it's interesting to point out  
10 that, in 2006, Federal Agencies were -- were asked to  
11 encrypt the data; and, a study that was done last year  
12 found that only 30% of -- of the agencies -- 30% of the  
13 data had been encrypted; and, in some cases, the  
14 devices that people thought had been encrypted were not  
15 -- had not been done.

16 And, that was found in a study that was  
17 done last year by the GAL Office.

18 If we are to meet the underlying goal of  
19 these Regulations, it is preferable to implement  
20 carefully designed and sustainable solutions; but, this  
21 will take time.

22 AICUM and its member institutions are  
23 committed to protecting the personal information of  
24 their students, employees and alumni.

1                   We applaud Governor Patrick,  
2                   Undersecretary Crane for pursuing this important public  
3                   policy; but, we believe more time will offer a better  
4                   set of standards and more reasonable time frame for  
5                   compliance.

6                   We would echo and support the comments  
7                   by Jon Hurst and the recommendations he made regarding  
8                   the offering another period for public comment and  
9                   reissuance of the standards and a two (2) year period  
10                  to comply and implement.

11                  Thank you, again, for this opportunity.

12                  HEARING OFFICER MURRAY: Thank you.

13                  I'm not sure I can read this name.  
14                  Newbury College?

15                  You're the one. Okay

16                  GERRY HAMMON: I'll have to practice my  
17                  penmanship. Thank you, Mr. Murray.

18                  ---

19                  **Gerry Hammon**

20                  **Newbury College**

21                  My name is Gerry Hammon, H-A-M-M-O-N.  
22                  I'm the Chief Information Officer at Newbury College.  
23                  I'm also on the Board of the Boston Society for  
24                  Information Management.

1                   Newbury College is a small Liberal Arts  
2 College in Brookline, Massachusetts, with about a  
3 thousand students.

4                   And, we have, essentially, all of the  
5 systems any large institution would have; however, I,  
6 actually, on have three (3) Staff --

7                   COURT REPORTER CYR: Excuse me. I'm sorry.

8                   Could someone, please, close that door.  
9 Please! Thank you.

10                  I'm sorry. They were running right over  
11 you.

12                  HEARING OFFICER MURRAY: Thanks. I'm sorry.  
13 My apologies.

14                  GERRY HAMMON: We have, essentially, all of  
15 the systems any large institution has because we have  
16 to do all the same functions and we have a large enough  
17 student body that it requires automation; but, I only  
18 have three (3) Staff where other institutions have --  
19 have many more Staff.

20                  So, we, definitely, support the goals  
21 that are in the Regulations.

22                  And, security is actually like a  
23 constant discussion daily both within information  
24 technology and with the business area; so, it

1 definitely is a concern.

2 And, we spend a lot of time actually  
3 implementing security and have already, for these  
4 Regulations, spent some time in public seminars.

5 So, we -- we take it very seriously;  
6 but, my biggest concerns are actually the -- the time  
7 frame and the costs associated with them; and then,  
8 finally, vendor certification which has been mentioned.

9 Developing comprehensive, written  
10 security policies, is a -- seems to be a very onerous  
11 task for us.

12 We've been evolving these policies; but,  
13 having a date-certain to implement -- to have those all  
14 ready require extensive resources from my Staff and  
15 with the business areas which are the key folks that  
16 know where the -- where all the data is, where all of  
17 the records are.

18 So, we need to -- We need, essentially,  
19 time to do that.

20 The -- Many of the systems that we  
21 actually have in place, we know do not -- they're  
22 vendor systems that do not have the features -- some of  
23 the features that are listed in the Regulations so we  
24 would have to -- if the requirement stands, those we'd

1 have to request vendor change; again, there's more cost  
2 associated with that; and, I'm not even sure what our  
3 vendors' reaction would be to that.

4 The whole area of encryption to me is  
5 certainly a goal to -- to work toward; but, for us,  
6 that would mean that we would have to -- I would have  
7 to train my IT Staff to really understand encryption  
8 and implement it and help the entire operation  
9 implement it.

10 And, certainly, we know that all the  
11 users of the technology definitely don't understand it  
12 and we're very concerned that our system -- that they  
13 wouldn't accommodate it and our systems might not even  
14 accommodate it.

15 And, finally, I guess the -- It has  
16 been brought up before. -- the -- the issues of vendor  
17 certification. We have quite a number of --

18 One of our strategies to survive with a  
19 lean Staff is to out-source and rely on other vendors  
20 from other -- other areas and a lot of those vendors,  
21 we're not sure that they're compliant and -- and the  
22 opportunity to find out about their compliance would be  
23 quite difficult for us.

24 So, again, I, really, thank you for the

1 opportunity to inform this committee today.

2 HEARING OFFICER MURRAY: Thank you.

3 That's the end of my Speaker's List. Is  
4 there any other comment that anyone wants to make that  
5 we haven't already heard?

6 [No Response]

7 Okay. Well, thank you all for coming.

8 The Hearing is closed.

[WHEREUPON, the Public Hearing was concluded at  
3:30 p.m.]

## C E R T I F I C A T E

## COMMONWEALTH OF MASSACHUSETTS

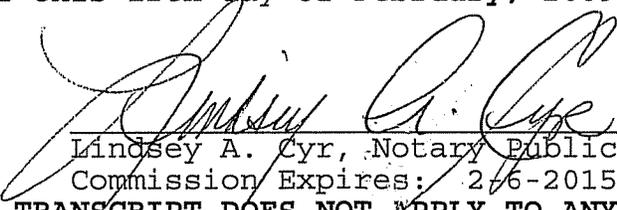
Norfolk, ss.

I, Lindsey A. Cyr, a Notary Public and Court Reporter in and for the Commonwealth of Massachusetts, do hereby certify that the foregoing Public Hearing of the **Office of Consumer Affairs & Business Regulation** was taken before me on **Friday, January 16, 2009**.

Said Public Hearing was taken audiographically by myself and then transcribed under my direction. To the best of my knowledge, the within transcript is a complete, true and accurate record of said Public Hearing.

I am not connected by blood or marriage with any of the said parties nor interested, directly or indirectly, in the matter involved in the Hearing.

IN WITNESS WHEREOF, I have hereunto set my hand and Notarial Seal this **12th** day of **February, 2009**.

  
Lindsey A. Cyr, Notary Public  
Commission Expires: 2-6-2015

**CERTIFICATION OF THIS TRANSCRIPT DOES NOT APPLY TO ANY REPRODUCTION OF SAME BY ANY MEANS UNLESS UNDER DIRECT CONTROL AND/OR SUPERVISION OF THE CERTIFYING REPORTER.**

<p><b>\$</b></p> <p><b>\$10,000.00</b> 55:5  <b>\$10Trillion</b> 31:10  <b>\$2.4Trillion</b> 31:19  <b>\$2.7Billion</b> 61:23  <b>\$290Billion</b> 31:16  <b>\$3.00</b> 68:2  <b>\$50,000.00</b> 55:8  <b>\$5Million</b> 72:5</p> <hr/> <p><b>0</b></p> <p><b>02116</b> 1:16; 2:5  <b>02191</b> 1:21</p> <hr/> <p><b>1</b></p> <p><b>1</b> 3:16,25; 7:6,7; 9:1; 10:20; 15:4; 16:17,21; 17:11,17,18; 19:16,16,18,21; 22:18,19; 29:17; 31:14; 36:9; 44:12; 48:11; 53:4,15; 55:9; 63:1,20; 65:7,17; 66:20; 68:5; 69:4; 70:17; 72:5; 84:9  <b>1-2</b> 1:2  <b>1-92</b> 1:1  <b>1/2</b> 24:22  <b>10</b> 1:16; 2:4,11; 8:9; 54:3; 56:15; 63:20  <b>10%</b> 61:24  <b>100,000</b> 81:18  <b>10th</b> 33:14  <b>12th</b> 34:10; 92:18  <b>1350</b> 10:23  <b>14th</b> 6:13; 8:5  <b>15</b> 4:6; 66:16  <b>150</b> 66:16  <b>16</b> 1:16; 2:13; 5:3; 92:8  <b>1600</b> 45:1  <b>16th</b> 8:7  <b>17</b> 1:3; 6:22; 33:20  <b>17.00</b> 1:7,9; 3:16; 6:11; 7:23; 8:16; 9:3; 45:5; 64:19  <b>17.02</b> 13:8  <b>17.03</b> 13:18; 14:2  <b>17.03(f)</b> 8:21  <b>17.04</b> 8:24; 12:7  <b>1700</b> 73:12  <b>17th</b> 33:19; 34:5; 35:12  <b>18</b> 37:11  <b>1988</b> 62:24  <b>19th</b> 33:24  <b>1:56</b> 1:17  <b>1st</b> 7:2,3; 36:6,11,15; 38:12,13; 45:9,10; 47:3; 48:14; 57:23; 58:6</p> <hr/> <p><b>2</b></p> <p><b>2</b> 3:20; 6:6; 8:6; 22:12; 23:17; 24:22; 30:18; 36:2,17,20; 40:21; 42:19; 48:9,18; 50:15; 62:9; 66:18; 72:6; 87:9  <b>2-6-2015</b> 92:21  <b>2.4Million</b> 70:16  <b>20</b> 63:7  <b>20%</b> 31:23  <b>2001</b> 72:10  <b>2006</b> 86:10</p>	<p><b>2008</b> 7:10,10; 8:5; 33:14,16  <b>2009</b> 1:17; 4:7; 5:3; 7:7; 8:7; 9:1,10; 10:20; 47:3; 56:7; 92:8,18  <b>201</b> 1:7,9; 3:16; 6:11,22; 7:23; 8:16,21,23; 9:3; 45:5; 64:19  <b>2010</b> 7:7; 8:18; 36:9; 38:13; 45:10; 71:19; 84:9  <b>21%</b> 31:19  <b>21st</b> 9:10  <b>22</b> 1:20  <b>23</b> 2:15  <b>24th</b> 34:17  <b>250</b> 66:23  <b>250,000</b> 81:17  <b>26th</b> 34:4,18  <b>28th</b> 7:10</p> <hr/> <p><b>3</b></p> <p><b>3</b> 22:12; 48:9; 55:12; 65:23; 66:18; 70:17; 88:6,18  <b>30</b> 57:24  <b>30%</b> 86:12,12  <b>30A</b> 3:21; 6:21; 7:14  <b>31</b> 2:17  <b>318</b> 54:4  <b>33,000</b> 31:23</p> <hr/> <p><b>4</b></p> <p><b>4</b> 3:19; 12:2; 17:22; 21:7; 54:4; 82:8  <b>40</b> 16:11  <b>44</b> 2:19  <b>49</b> 25:10; 26:10</p> <hr/> <p><b>5</b></p> <p><b>5</b> 8:8; 12:12; 46:23; 72:11  <b>5)</b> 8:24  <b>5-6</b> 1:15  <b>50</b> 16:11; 31:9; 53:9; 60:17; 72:4  <b>500</b> 54:14  <b>501-C(3)s</b> 61:19  <b>504</b> 77:22  <b>51</b> 2:22  <b>5170</b> 2:4  <b>52</b> 2:24  <b>5500</b> 62:6  <b>59</b> 81:14</p> <hr/> <p><b>6</b></p> <p><b>6</b> 2:9; 3:19; 8:8; 56:3  <b>61</b> 3:2  <b>64</b> 3:4  <b>6500</b> 51:7</p> <hr/> <p><b>7</b></p> <p><b>7</b> 46:21  <b>70</b> 3:6; 23:19  <b>73</b> 3:8  <b>781-337-4638</b> 1:22</p> <hr/> <p><b>8</b></p>	<p><b>8</b> 7:10  <b>80%</b> 54:6  <b>81</b> 3:10  <b>85%</b> 46:22  <b>87</b> 3:12  <b>8th</b> 33:16</p> <hr/> <p><b>9</b></p> <p><b>9</b> 3:25  <b>90</b> 67:19; 68:2  <b>93A</b> 30:6  <b>93H</b> 3:25; 7:19; 33:8; 38:19,24; 43:23  <b>93I</b> 67:15  <b>93Million</b> 31:11</p> <hr/> <p><b>A</b></p> <p><b>abilities</b> 62:4  <b>ability</b> 27:24  <b>able</b> 17:10; 43:9; 46:24; 58:5,7  <b>absence</b> 25:24; 36:4  <b>absolutely</b> 63:8,13; 71:7; 73:23  <b>Abuse</b> 62:3  <b>accelerating</b> 80:9  <b>accept</b> 12:24  <b>acceptable</b> 21:9  <b>accepted</b> 9:8  <b>access</b> 55:18; 56:12  <b>accidently</b> 58:14  <b>accommodate</b> 90:13,14  <b>accommodated</b> 77:9  <b>accompany</b> 14:11  <b>accomplish</b> 19:10; 36:6  <b>accordance</b> 41:17  <b>Accordingly</b> 37:5  <b>account</b> 31:15; 59:1,5; 74:14,17,18,22  <b>accounts</b> 37:4  <b>accurate</b> 92:12  <b>achieved</b> 75:17  <b>achieves</b> 44:9  <b>acknowledge</b> 28:10; 73:20  <b>acquire</b> 69:11  <b>across</b> 12:9; 45:2; 49:1; 62:6; 84:21  <b>Act</b> 83:8  <b>action</b> 25:24; 30:5,15  <b>actions</b> 53:20; 58:21  <b>activities</b> 34:14  <b>activity</b> 30:8; 62:20  <b>actually</b> 23:2; 51:12; 64:15; 68:20; 72:12; 75:1; 88:6,22; 89:2,6,21  <b>add</b> 37:9; 83:5  <b>Adding</b> 75:6  <b>addition</b> 80:12  <b>additional</b> 40:21; 50:7; 56:17,18; 68:12; 83:5,11,12  <b>Additionally</b> 44:4  <b>address</b> 20:19; 22:7,10; 32:24; 34:19,19; 35:10; 40:4; 79:13; 85:12  <b>addressed</b> 4:7; 5:10,16; 52:4; 74:2  <b>addresses</b> 13:15; 72:17  <b>adequate</b> 20:4,21  <b>adequately</b> 14:7</p>	<p><b>adhere</b> 17:20  <b>Administration</b> 11:6,16; 45:13; 48:15; 52:15; 73:16  <b>administrative</b> 58:9  <b>Administrators</b> 42:7  <b>adopt</b> 33:2; 43:10; 48:15  <b>adopted</b> 13:14; 37:23  <b>adopting</b> 41:21; 44:8  <b>adoption</b> 33:15; 41:17; 42:12; 44:5; 62:3  <b>advancing</b> 11:15  <b>adverse</b> 29:22  <b>advertising</b> 79:5  <b>advice</b> 18:20; 20:2,19; 22:17; 43:18  <b>Advisory</b> 20:7,22; 21:6,14,21; 52:8  <b>AeA</b> 2:11; 4:3; 10:15,17,19; 11:10; 12:2  <b>AFFAIRS</b> 1:5; 2:3,21; 3:24; 4:18,21; 5:17; 6:8; 7:17,19; 9:13; 11:2; 14:23; 33:6; 44:21; 92:7  <b>affected</b> 42:10; 54:12  <b>affects</b> 55:13  <b>affiliation</b> 16:10  <b>affirm</b> 39:6  <b>affirmative</b> 82:2  <b>afford</b> 8:12  <b>afforded</b> 9:5  <b>aforementioned</b> 8:15  <b>afternoon</b> 23:11; 38:6; 44:19; 73:8; 81:5,6,21; 82:5  <b>afternoon!</b> 10:16; 52:24; 61:7  <b>again</b> 33:21; 34:15; 35:4; 47:14; 48:14; 49:7,18; 50:9; 57:20; 58:9; 66:10; 72:24; 80:22; 85:14; 87:11; 90:1,24  <b>Against</b> 21:1  <b>Agencies</b> 20:6; 22:6; 45:2,7,12,23; 46:10,14,20,22,24; 47:16; 48:10,21; 53:9; 77:22,23; 86:10,12  <b>Agency</b> 18:2,14,18; 20:1,18; 26:14; 30:16; 46:21; 49:23; 75:15; 76:4; 80:23  <b>Agency's</b> 78:11; 79:13  <b>Agent</b> 69:16  <b>Agents</b> 2:19; 4:17; 44:18,23  <b>aggressive</b> 33:18,23  <b>agree</b> 28:9; 51:15; 75:19  <b>ahead</b> 80:17  <b>AICUM</b> 3:10; 5:2; 81:9,12,14; 84:11,18; 86:22  <b>aid</b> 83:1  <b>AIM</b> 2:24; 52:23; 53:4,5  <b>AIM's</b> 51:15,24  <b>akin</b> 60:3  <b>aligning</b> 36:20  <b>alike</b> 25:3  <b>allow</b> 24:23; 27:15; 30:4  <b>allowance</b> 80:3  <b>allowances</b> 77:21  <b>allowed</b> 77:23  <b>allowing</b> 50:20; 76:5  <b>almost</b> 16:23; 31:10,11  <b>alone</b> 54:7</p>
---	---	---	---

along 16:5; 33:20  
**already** 18:9; 21:19; 22:8; 39:11; 41:20; 50:2; 57:21; 71:4; 75:7; 82:1,4; 94:1,12,23; 89:3; 91:5  
**alternative** 69:9  
**Although** 45:8  
**alumni** 82:3; 85:1; 86:24  
**ambiguous** 40:17  
**Amended** 3:16; 6:15,18; 8:3; 9:14; 81:21  
**Amendment** 40:13  
**Amendments** 6:11,21; 7:2,22; 8:15,17  
**America** 4:3; 5:21; 10:21  
**American** 5:24; 10:19  
**among** 40:2; 53:14; 80:13,14  
**amongst** 71:9  
**amount** 17:10; 38:21,22; 55:8; 65:21; 68:21; 69:10; 79:2; 84:6; 85:8  
**ample** 44:5  
**amply** 40:18  
**Analysis** 4:4; 41:5,16; 45:15; 47:21,24; 49:20; 50:12; 56:14; 67:23  
**and/or** 16:17; 92:24  
**Andrea** 2:23; 52:20,22; 53:1; 59:20,22  
**Andrew** 5:18  
**anecdotally** 72:19  
**ANGELL** 2:13; 16:2,4  
**Ann** 3:5; 4:25; 69:24; 70:1,4,8,10,11  
**Anne** 2:10; 4:2; 10:12,14,16; 15:16,18  
**answer** 40:7  
**anxious** 15:7  
**anymore** 85:4  
**anyone** 10:1; 24:18; 35:17; 91:4  
**anything** 25:20  
**anytime** 30:8  
**anyway** 60:11  
**apologies** 59:21; 88:13  
**appear** 16:21; 38:15; 39:8  
**appearance** 33:10  
**appeared** 14:13  
**appears** 35:17  
**applaud** 81:23; 87:1  
**applicability** 28:20; 60:14; 61:1  
**applicable** 1:11; 30:14  
**application** 12:18; 34:14  
**applied** 28:23  
**apply** 56:2; 92:22  
**appreciate** 45:3; 51:12; 52:10; 69:21; 70:19; 79:12  
**appreciative** 71:3  
**approach** 14:14; 39:23; 42:17; 43:19; 47:9; 49:19; 75:20; 76:5  
**appropriate** 33:2; 37:6; 38:9,10,13  
**appropriated** 63:2  
**appropriately** 43:24  
**appropriateness** 35:15  
**approximately** 31:13,15,23; 37:11; 46:22; 61:24; 81:18  
**arbitrary** 85:21

**archive** 18:21  
**area** 84:17; 85:22; 88:24; 90:4  
**areas** 82:9; 89:15; 90:20  
**aren't** 9:17; 26:8; 29:8,22  
**arguably** 24:18  
**argue** 65:6  
**argument** 27:21  
**around** 28:4,4; 63:19  
**Arts** 88:1  
**ask** 10:10; 21:20; 71:18; 75:20; 76:4; 77:5,9; 78:4; 79:7  
**asked** 35:12; 64:19; 86:10  
**asking** 62:7; 64:22  
**assets** 31:10,16,19,20; 72:5  
**assistance** 20:4  
**Assoc** 2:21  
**Associate** 4:20  
**Associated** 2:22; 4:19; 5:1; 51:5,7; 89:7; 90:2  
**ASSOCIATES** 1:19  
**Association** 2:15,19; 4:3,12,16; 5:8,9,15,21,24; 10:20,21,22; 16:8; 21:5,17,18; 23:10,13; 24:3; 31:7; 34:11; 44:18,22,24; 45:1; 46:19; 50:16; 61:18; 70:14; 81:12  
**Association's** 45:4  
**assume** 12:15; 56:15  
**assuming** 22:19  
**assurances** 84:7  
**attached** 5:23; 32:7; 35:9  
**attempts** 60:22; 65:9  
**attend** 10:10; 81:17  
**attended** 85:17  
**attending** 34:10  
**attention** 9:13; 11:6; 79:24  
**Attorney** 2:23; 11:5; 20:13,16; 22:4; 29:23,24; 30:13; 45:17; 50:10; 52:22; 53:2; 59:20,22  
**attorneys** 27:23  
**audiographi-** 92:9  
**authority** 3:22; 7:15; 38:17; 39:11,13  
**automation** 88:17  
**available** 12:18; 13:3; 17:12; 18:22; 47:5; 80:5  
**average** 46:21  
**aware** 17:15,19; 37:21; 80:15  
**awareness** 66:7; 80:12

**B**

**B-E-R** 16:4  
**back** 20:17; 25:14; 27:13; 29:10; 42:7; 44:14; 65:11  
**back-up** 19:6,7  
**background** 34:22  
**bad** 29:12  
**balance** 43:24; 46:1; 54:19  
**balanced** 42:17  
**Bankers** 5:8  
**Bar** 16:8; 21:5,7,17,18; 22:12  
**based** 37:16; 38:20; 47:4; 76:6; 80:4

**basically** 63:16  
**basis** 6:13; 16:24; 28:16; 30:19; 75:3; 77:20; 78:1  
**became** 6:13  
**become** 38:6  
**becoming** 24:7  
**Beetles** 60:5  
**begun** 37:18  
**behalf** 16:13; 34:7; 44:24; 54:16,17; 60:12; 70:10; 73:12  
**believe** 17:9; 26:17; 27:6; 28:7; 30:3,15; 38:10; 41:3; 42:13; 45:11,24; 46:6; 47:8; 49:13; 50:4; 74:2; 79:16,21; 87:3  
**believes** 36:5,8; 37:17; 41:4; 50:5  
**benefit** 10:2; 54:18  
**benefits** 55:9; 58:24  
**Best** 76:14; 92:11  
**better** 14:19; 18:3; 22:20; 79:21; 87:3  
**beyond** 46:7; 48:23; 56:8; 59:24; 86:1  
**big** 68:3  
**biggest** 89:6  
**Bill** 5:13  
**bit** 65:12  
**Blackberries** 19:4  
**blood** 92:14  
**Blyley** 26:7  
**Board** 21:14; 42:8; 87:23  
**Boards** 20:7,22  
**Bob** 81:4  
**body** 88:17  
**boiled** 68:19  
**Boston** 1:16; 2:5; 3:8; 4:26; 7:10; 16:8; 21:17; 49:23; 73:7,10; 87:23  
**Bottom** 14:5; 24:4  
**bought** 27:11  
**Bounty** 30:7  
**Box** 1:20  
**Brad** 50:23,24; 51:6  
**Bradley** 2:20; 4:20; 51:1,4  
**brand** 32:15  
**breach** 30:8; 53:19  
**breaches** 29:2,2,3; 46:5; 53:22; 54:3,4,6,11,14; 60:2  
**break** 22:24  
**breathes** 68:7  
**brief** 11:18; 13:20; 23:14; 25:7; 51:2  
**briefly** 33:13; 40:20; 82:8  
**bringing** 70:24  
**broad** 19:11  
**broad-based** 11:22  
**Brookline** 88:2  
**brought** 71:22; 90:16  
**Budget** 61:24  
**budgetary** 80:9; 83:4  
**budgets** 63:8  
**Building** 1:15; 8:9; 63:6  
**bulk** 54:13  
**bullet** 65:3  
**burden** 66:11; 80:10; 83:11  
**burdens** 50:7  
**burdensome** 42:3  
**BUSINESS** 1:5; 2:3; 3:24; 5:14,17; 6:9; 7:17,20; 9:9;

11:22; 12:1; 14:8,23,24; 15:11; 27:6,10,22; 28:3,8; 33:7; 37:21; 38:21; 43:2,2; 44:3; 46:3,12,17; 47:6,10; 48:2,16,24; 49:8; 50:8; 51:23; 53:7,8,11; 54:23; 55:19; 56:10; 57:12; 58:7,14; 59:5,9; 65:16; 66:11; 69:14; 71:12; 78:23; 79:10; 80:5; 82:20; 84:15; 88:24; 89:15; 92:7  
**business'** 57:14  
**businesses** 13:4; 27:15; 28:5; 41:11; 44:1; 50:1; 53:18,23; 54:5,10; 55:2,13; 58:4; 59:9; 60:8,13,16,17; 61:1; 69:10; 79:14,18,19,23  
**buy** 66:22; 69:15  
**Buyse** 5:11

**C**

**C-L-A-N-C-Y** 70:12  
**cabinets** 56:16,21  
**Calamare** 5:18  
**calculated** 55:7  
**Calendar** 71:19  
**Call** 26:13  
**called** 69:8  
**calling** 11:2  
**cally** 92:10  
**campus** 84:22  
**can't** 20:1,20; 27:13; 29:13; 74:19  
**capabilities** 75:6  
**capable** 18:15  
**card** 58:16  
**cards** 71:10  
**care** 59:18  
**carefully** 86:20  
**Caring** 4:22  
**carried** 50:15  
**carriers** 49:1  
**carry** 21:12  
**case** 71:1  
**cases** 13:3; 76:23; 86:13  
**Casualty** 5:20  
**category** 74:10,24; 76:9; 78:20; 79:9; 83:14  
**caught** 68:1  
**caused** 65:20  
**cellphone** 10:11  
**cellphones** 59:19  
**certain** 6:11,24; 7:4,5; 12:23; 17:10; 28:13; 69:10; 78:13  
**certainly** 29:18,19,23; 30:13; 48:3; 63:22; 70:19,23; 72:17; 90:5,10  
**certainty** 40:10  
**certification** 8:19; 19:17,19; 28:15; 48:20; 49:5,10; 76:10; 77:6,14,19; 78:8; 83:16; 89:8; 90:17; 92:22  
**certifications** 36:8; 39:18; 77:15  
**certify** 77:3,24; 78:17; 83:19; 92:6  
**CERTIFYING** 92:24  
**chair** 16:4; 21:8  
**Chairman** 72:2  
**Chamber** 3:8; 4:26;

<p>73:7,10,11,18; 80:16  <b>Chambers</b> 23:19  <b>change</b> 90:1  <b>changes</b> 13:10; 54:23; 91:2; 83:8  <b>Chapter</b> 3:21,25; 6:21; 7:14,18; 33:8; 38:19,24; 43:23  <b>check</b> 66:19,22  <b>check-box</b> 68:17,20  <b>check-out</b> 58:18  <b>checklist</b> 69:17; 79:10,11,17,21  <b>Chief</b> 5:19; 87:22  <b>CISM</b> 4:8  <b>CISSP</b> 4:8  <b>cited</b> 74:12  <b>Cities</b> 28:23; 29:14  <b>Citizen</b> 65:18  <b>Civil</b> 54:8  <b>civilly</b> 59:13  <b>Clancy</b> 3:5; 4:25; 70:1,4,8,10,12  <b>clarification</b> 29:24; 34:9  <b>Clause</b> 39:7; 79:8  <b>clear-cutting</b> 60:3  <b>clearer</b> 59:8  <b>clearly</b> 34:22; 51:9,15; 52:3,6  <b>client</b> 16:13; 54:17  <b>clients</b> 49:1; 53:6,12; 54:8,16; 57:1; 59:9  <b>close</b> 6:6; 9:9; 26:6; 88:8  <b>closed</b> 91:8  <b>Closed]</b> 64:5  <b>closing</b> 40:20; 80:7  <b>CMR</b> 1:7,9; 3:16; 6:11,22; 7:23; 8:16,21,24; 9:3; 45:5; 64:19  <b>co-chair</b> 16:7,9  <b>Coakley</b> 11:5  <b>coalition</b> 11:23; 15:11; 48:2,5,16; 49:8; 51:23  <b>Codes</b> 63:6  <b>codified</b> 75:20  <b>codifying</b> 78:12  <b>collaborative</b> 47:17  <b>collected</b> 79:2  <b>collection</b> 78:21,22  <b>College</b> 3:12; 87:14,20,22; 88:1,2  <b>Colleges</b> 5:2; 81:12,15,22; 82:1,7,13,21; 83:9,20; 84:18,23  <b>comes</b> 17:9; 25:20; 82:19  <b>coming</b> 58:6; 61:10; 66:18; 91:7  <b>commence</b> 8:6  <b>commencing</b> 1:17  <b>commend</b> 11:16  <b>commendable</b> 70:24; 71:15  <b>commended</b> 59:24  <b>comment</b> 18:18; 33:8; 37:19,20; 42:10,22; 45:16; 81:21; 87:8; 91:4  <b>comments</b> 9:8,11; 11:19; 15:4,5; 16:22; 21:19; 24:2; 40:11; 58:2; 72:24; 82:4; 87:6  <b>Commerce</b> 3:8; 4:26; 23:20; 25:21; 39:2,7;</p>	<p>73:7,10  <b>commercial</b> 62:20  <b>Commission</b> 20:9,24; 92:21  <b>Commission's</b> 36:13  <b>Commissioner's</b> 22:13  <b>commit</b> 47:1  <b>commitment</b> 33:3; 76:16  <b>commitments</b> 76:16  <b>committed</b> 11:10; 86:23  <b>Committee</b> 4:9; 16:7; 21:6,17,22; 34:1; 91:1  <b>common</b> 65:5,8,9  <b>commonly</b> 80:19  <b>COMMONWEALTH</b>  1:4,11,14; 3:19; 31:12,22; 32:4; 39:4; 45:2; 50:6; 61:23; 62:6; 63:21; 65:18,22; 68:22; 70:15; 92:2,5  <b>Commonwealth's</b>  39:5,10; 55:22  <b>communicated</b> 51:10  <b>Communities</b> 4:23; 47:18  <b>Community</b> 12:1; 13:14; 14:24; 42:14; 43:3; 45:18; 46:3; 50:11; 53:7  <b>Community-based</b> 62:15  <b>companies</b> 10:23; 11:10; 12:8,13; 16:24; 17:15,18; 18:8,23; 22:15,21; 23:1; 31:19,21; 33:21; 37:2,10; 41:11; 54:7,11; 57:21; 66:6,7,20; 67:2,5; 73:23; 74:13; 75:11; 76:1,5,11,18; 78:2,14,24; 79:6; 80:8  <b>companies'</b> 19:22  <b>Company</b> 2:17; 4:14; 12:6; 31:2,5; 56:1,15; 57:23; 64:15; 65:23; 78:7  <b>company's</b> 76:15  <b>competitive</b> 79:6  <b>competitiveness</b> 74:4  <b>complete</b> 75:24; 92:12  <b>complex</b> 20:18; 21:2; 37:14; 83:17; 86:3  <b>complexity</b> 38:14  <b>compliance</b> 6:24; 7:1,3,24; 8:18; 9:1; 24:23; 25:13; 26:19,21; 27:13; 28:15; 32:7; 33:18,23; 34:8; 35:9,13; 36:11,14,18,21; 37:7,8,11; 38:12; 39:17,19; 40:10; 47:4; 55:5; 58:8,10; 59:3,10,13; 60:17,22; 62:19; 68:19; 71:24; 72:22; 76:5; 77:3; 78:7; 79:10,10,15; 80:3,14; 83:13,19; 87:5; 90:22  <b>compliant</b> 19:18; 43:22; 73:24; 80:1; 90:21  <b>complicated</b> 20:1  <b>comply</b> 16:16,24; 36:9; 37:13; 44:6; 45:12; 47:2; 48:14; 62:13,16; 63:17,23; 82:17; 83:10; 85:7; 87:10  <b>component</b> 32:17; 67:3  <b>compounded</b> 63:13  <b>comprehensive</b> 55:16; 89:9  <b>comprising</b> 35:1  <b>compromise</b> 28:1  <b>compromises</b> 71:11</p>	<p><b>computer</b> 12:17; 54:9  <b>conceivably</b> 84:20  <b>concern</b> 34:8; 48:10,12,21; 82:9; 83:14; 84:17; 85:22; 89:1  <b>concerned</b> 29:18; 30:7; 74:14; 90:12  <b>concerning</b> 1:9  <b>concerns</b> 14:9; 23:21; 32:5; 33:5,12,14,17,21; 34:2,13,23; 35:5; 38:1,11; 40:12,14; 41:11; 42:6; 43:1,24; 45:4; 50:20; 51:14; 72:7,20; 73:1; 79:14; 89:6  <b>concise</b> 65:1  <b>concur</b> 43:13  <b>conduct</b> 48:24  <b>conducted</b> 41:17; 46:19  <b>conducting</b> 44:3  <b>conference</b> 34:11  <b>confidentiality</b> 32:11,18; 38:23; 62:14; 80:6  <b>confirm</b> 39:16  <b>conflict</b> 25:18  <b>conflicts</b> 25:8  <b>confusing</b> 19:21; 46:9; 49:7  <b>Congress</b> 26:15  <b>connected</b> 51:21; 92:14  <b>connection</b> 1:8; 6:10; 7:5,21  <b>consequence</b> 17:5,8,9  <b>consequences</b> 60:7  <b>consider</b> 18:21; 23:1; 43:18; 52:11; 76:4; 79:23  <b>considerable</b> 37:22; 84:6  <b>consideration</b> 23:18; 50:19; 71:18; 74:9; 77:5; 78:5; 79:7  <b>considered</b> 30:15; 46:17; 77:10  <b>consistency</b> 48:19,22  <b>consistent</b> 38:17; 42:1; 43:23; 77:20  <b>constant</b> 88:23  <b>Constitution</b> 39:8  <b>consult</b> 35:17  <b>consulted</b> 35:14  <b>consulting</b> 57:4; 66:15  <b>CONSUMER</b> 1:5; 2:3; 3:23; 4:9; 5:17; 6:8; 7:16,19; 9:12; 11:2; 14:23; 26:20; 32:12; 33:6; 34:1; 92:7  <b>Consumers</b> 12:1; 14:19; 70:17; 71:7  <b>consuming</b> 14:3; 49:17; 57:7; 76:23  <b>contain</b> 83:23; 84:1  <b>containing</b> 12:9; 55:18  <b>context</b> 35:5; 51:20; 57:11; 58:4  <b>continue</b> 11:18; 14:23; 15:8,12; 32:23; 41:1; 52:16; 83:2,2  <b>continued</b> 11:6; 12:4  <b>continues</b> 13:20  <b>continuing</b> 80:17  <b>contract</b> 28:10; 48:19; 49:5; 77:4,16; 78:9  <b>contracts</b> 13:21; 28:1; 39:15; 58:5,7; 61:22; 62:19; 63:5; 76:19,21; 83:21,24;</p>	<p>84:4  <b>contractual</b> 49:9; 76:11  <b>contractually</b> 57:23  <b>contrary</b> 39:7  <b>contrast</b> 14:12; 47:13; 55:21  <b>CONTROL</b> 92:24  <b>convened</b> 6:10; 85:9  <b>cooperative</b> 30:19  <b>coordinate</b> 85:6  <b>coordination</b> 21:4  <b>Copies</b> 6:15; 9:14,18  <b>Copy</b> 3:16,20; 6:17; 9:19; 38:6  <b>corporations</b> 23:20  <b>correspondence</b> 35:23; 38:2; 40:19  <b>cost</b> 54:18; 55:5; 56:8,14,22; 57:21; 58:10,22; 76:2; 79:18; 80:10; 82:11; 90:1  <b>costly</b> 13:23; 42:3; 49:16; 75:8; 76:22  <b>costs</b> 41:12; 54:24; 76:2; 82:14; 89:7  <b>Council</b> 2:11; 3:2; 4:22; 5:6; 10:15; 61:13,17  <b>Counsel</b> 2:2; 4:18; 5:22; 6:8  <b>counterparts</b> 25:10  <b>Countries</b> 16:11  <b>Country</b> 17:4; 28:4; 49:2  <b>couple</b> 27:12; 64:20; 65:15; 66:4  <b>Court</b> 1:13; 44:12; 64:4; 88:7; 92:4  <b>cover</b> 15:18  <b>covers</b> 72:9  <b>crafting</b> 14:19  <b>Cramer</b> 2:23; 52:20,22; 53:1; 59:20,22  <b>Crane</b> 4:7; 5:10,16; 11:2; 47:22; 70:21; 73:15; 81:24; 87:2  <b>create</b> 56:10  <b>created</b> 18:6  <b>creates</b> 46:8  <b>creation</b> 13:22  <b>credible</b> 41:16  <b>Credit</b> 3:6; 4:24; 58:16; 70:9,13,14,18; 71:9; 72:4,4,10  <b>crisis</b> 50:6; 82:22  <b>crowded</b> 11:8  <b>current</b> 43:16,20; 47:8; 48:22; 55:13; 62:16; 82:6  <b>currently</b> 46:6; 76:20; 82:10  <b>customer</b> 42:10; 53:16; 55:14; 58:15; 60:8,18; 74:14,18,22; 78:23; 79:5  <b>customer's</b> 76:13  <b>customers</b> 24:19; 54:21; 61:3; 66:15; 76:17  <b>cutting</b> 75:12  <b>Cyr</b> 1:13,19; 44:12; 64:4; 88:7; 92:4,20  <b>D</b>  <b>D-A-N-I-E-L</b> 64:14  <b>daily</b> 16:24; 88:23</p>
---	--	---	---

**Dan** 44:15,20; 50:22  
**Daniel** 2:18; 3:3; 4:7,17; 5:10,16; 44:17; 64:3,7,8,10,12  
**data** 12:10; 14:21; 29:2,3; 32:5; 33:3; 38:22; 39:23; 41:22; 42:17,20; 43:12,12; 48:3; 49:4,21; 51:16; 52:18; 54:2; 69:11; 71:6,11; 74:1; 76:3,6,7; 80:5,18; 83:22; 86:11,13; 89:16  
**date** 7:1,23; 8:18; 9:1; 19:20; 27:7,19; 32:7; 33:18,23; 34:8; 35:2,9,13; 36:11,14; 37:7,8; 41:6; 42:5; 45:8; 72:22; 75:4; 77:17  
**date-certain** 28:9; 89:13  
**dated** 4:6; 5:3; 33:16  
**dates** 6:24; 17:12; 35:18; 36:21; 38:12; 73:22  
**David** 2:2; 4:7; 5:7; 6:3,7; 15:23  
**day** 37:24; 92:18  
**days** 22:12; 79:20; 80:17  
**de** 41:2  
**deadline** 7:4; 36:19; 85:21  
**deadlines** 60:16; 82:6  
**deal** 27:5; 61:20; 83:6  
**dealing** 25:20; 76:10  
**December** 7:10; 33:9; 34:10,17; 40:13; 41:10  
**decision** 71:12; 73:21  
**deems** 37:6  
**deep** 57:6  
**deeper** 22:24; 65:12  
**defective** 16:15  
**defendants** 21:10  
**deferment** 6:24  
**deficiencies** 40:12  
**defined** 13:11; 45:21; 62:19  
**definitely** 88:20; 89:1; 90:11  
**definition** 13:7,9,13; 40:16  
**definitions** 74:10  
**degree** 40:9; 53:22  
**delay** 11:3,17; 52:16; 64:22; 73:21,22  
**delays** 74:5  
**deliberated** 17:7  
**deliberative** 14:14; 43:5  
**delivered** 4:17,20,23,25,27; 47:22  
**demand** 30:10  
**dents** 3:19  
**Department** 33:6,20; 34:5,6,15,16,18,23; 35:4,11,13,14,17; 36:5,10; 37:6,12,16,17; 40:15,19; 41:2,4; 43:17; 44:8; 45:17; 48:15; 50:10,17; 51:10,13,22,24; 52:17; 58:19  
**Department's** 35:8; 37:15; 38:16; 40:3; 41:15  
**departments** 84:22  
**depend** 52:5  
**depends** 32:16  
**deployed** 13:3  
**deployment** 67:9  
**derives** 32:13

**Description** 3:15  
**descriptive** 81:1  
**designed** 84:1; 86:20  
**destruction** 67:15  
**detail** 34:12; 38:4  
**detailed** 22:15,17  
**details** 55:11  
**determination** 35:21  
**determine** 35:14  
**determined** 35:13,18  
**detrimental** 52:12; 53:20  
**devastating** 45:5; 46:14  
**develop** 23:23; 85:10,12  
**developed** 21:8,16  
**developing** 17:20; 89:9  
**devices** 8:22; 12:14; 36:7; 86:14  
**devices"** 19:3  
**dialog** 26:5  
**dialogue** 11:9,18; 15:8; 23:23; 35:4; 43:20  
**didn't** 75:15  
**difference** 19:16  
**different** 24:14; 58:15; 69:6  
**difficult** 22:7; 39:24; 67:4; 75:8; 82:20; 84:16; 90:23  
**difficulty** 40:1  
**dig** 65:12  
**diligence** 83:18  
**Direct** 5:13; 35:23; 83:1; 92:23  
**directed** 6:23  
**direction** 69:2,6; 74:6; 92:11  
**directly** 24:2; 51:10; 78:9; 92:15  
**Director** 2:10; 3:23; 4:2; 5:17; 7:16; 10:17; 61:16; 70:21; 73:9  
**disabilities** 62:5  
**disadvantage** 26:4,9; 28:5; 79:6  
**disagree** 35:20; 58:3  
**disclosed** 58:14  
**Discovery** 57:13  
**Discrimination** 21:1  
**discuss** 32:6  
**discussed** 34:12; 75:23  
**discussion** 12:5; 74:8; 80:17; 88:23  
**discussions** 12:4; 47:17  
**disposal** 67:16  
**disproportionately** 54:12  
**disputes** 57:12  
**disrupting** 79:3  
**distinct** 79:6  
**distinguish** 53:16  
**distributed** 84:21  
**dive** 22:23  
**diverse** 13:1  
**doable** 58:10; 68:15  
**Document** 5:5; 67:14  
**documented** 38:2; 63:14  
**documents** 23:18; 40:18; 56:13; 57:3,19; 83:23  
**DODGE** 2:13; 16:2,4  
**does** 25:17; 46:9; 52:5; 56:2; 58:23; 67:15,22; 92:22  
**doesn't** 49:12  
**Doherty** 2:10; 4:2; 5:3;

10:12,14,16; 15:16,18  
**doing** 27:16,18; 62:9; 84:9  
**dollars** 32:22; 41:8; 56:23  
**domestic** 62:2  
**done** 18:8; 20:23; 25:23; 41:6; 66:17; 69:18; 70:24; 71:4; 72:2; 86:11,15,17  
**donors** 85:1  
**door** 88:8  
**doors** 27:3; 56:17; 57:2  
**down** 57:21; 65:3,24; 67:20; 68:19  
**drawing** 21:16; 42:8  
**Drives** 19:5  
**drop** 28:9,17  
**due** 58:6; 76:2; 83:18  
**duplication** 25:7  
**during** 54:3; 60:21  
**dwelling** 38:4

**E**

**ease** 67:8,9  
**easy** 68:10  
**echo** 87:6  
**echoing** 82:4  
**economic** 40:23; 79:20  
**economy** 26:24; 27:3; 29:13; 46:20; 51:8; 52:5,13; 55:1; 57:21; 63:12; 80:21  
**edge** 75:12  
**educate** 25:16  
**education** 13:23; 24:9,23; 25:1,6; 29:20; 83:2,7  
**EDWARDS** 2:13; 16:2,4  
**effect** 16:21; 53:20  
**effected** 24:17  
**effecting** 24:14  
**effective** 6:13; 40:1; 44:9; 45:8; 73:22; 75:4; 77:17  
**effects** 24:18  
**effectuate** 52:17  
**efficiency** 36:18; 57:20  
**effort** 23:2; 60:9; 68:21; 81:24  
**efforts** 34:22; 35:2; 70:23; 71:15; 79:15; 80:23  
**either** 9:15; 34:19; 57:16; 68:16  
**elected** 10:5; 45:19; 50:11  
**electronic** 56:12  
**Electronics** 10:19  
**elements** 22:24  
**eliminate** 77:12  
**eliminating** 58:23  
**eloquently** 66:9  
**else** 62:22  
**elsewhere** 13:5; 24:1  
**emergency** 6:12; 8:4; 33:8; 35:6; 40:13; 41:20  
**emerging** 33:1  
**empirical** 36:5  
**employed** 75:19; 81:19  
**employee** 53:17; 60:15; 66:16  
**employee's** 55:9; 57:13,14  
**employees** 24:19; 31:24; 46:21,23; 53:9; 55:17; 56:3; 60:17; 66:23; 72:6; 82:3; 85:1; 86:24  
**employer** 55:23  
**employers** 18:23; 25:3;

26:8; 27:2; 29:12; 31:22; 53:17; 54:19; 56:2,4; 80:13,14  
**employing** 31:22; 75:11  
**Employment** 53:2; 57:11; 60:23  
**employs** 46:21  
**enable** 36:11; 75:18  
**enact** 84:13  
**encourage** 14:22  
**encrypt** 12:8,10,13,20; 86:11  
**encrypted** 39:14; 86:13,14  
**encrypting** 8:22  
**encryption** 7:4; 12:16,23; 13:7; 27:4; 36:7; 40:16; 49:11; 66:10,11,13,17; 67:2,7; 72:15; 74:24; 75:2,6,10,17; 85:23; 86:7; 90:4,7  
**end** 79:3; 91:3  
**endowments** 82:23  
**energy** 37:22; 49:24  
**enforce** 29:23  
**enforceable** 30:13  
**enforcement** 29:18,21; 39:11  
**enforces** 30:1  
**engage** 45:14; 47:23; 50:12; 73:18  
**engaged** 15:12; 18:9; 47:17; 50:17  
**engaging** 27:23; 43:20; 78:14  
**Engineering** 54:8  
**England** 2:11; 10:15,18  
**enormous** 65:21  
**enough** 6:6; 9:18; 63:18; 66:19; 88:16  
**ensure** 32:24; 43:11; 44:4; 46:4; 58:8; 74:22  
**Ensuring** 74:1  
**entails** 18:7  
**entered** 6:18; 9:20  
**enterprises** 67:10  
**entire** 45:16; 50:13; 54:18; 57:17; 73:16; 90:8  
**entities** 28:2,21; 29:4  
**entitled** 5:5  
**entity** 16:13; 30:9  
**epicenter** 31:17  
**equally** 11:13  
**equipment** 27:12; 64:17; 75:4  
**eradicate** 60:4,10  
**especially** 46:14; 47:15; 65:24; 76:23  
**Esquire** 2:12; 16:1  
**essential** 63:19; 73:23; 76:15  
**essentially** 82:12; 88:4,14; 89:18  
**establish** 74:19  
**estimate** 55:5  
**evaluating** 86:7  
**eventually** 56:5  
**everybody** 24:17  
**everyone** 9:23; 10:10; 49:2; 59:18; 70:21  
**everything** 28:17,18; 69:17  
**evidence** 36:5

evolving 12:24; 75:13;  
 76:3,3; 89:12  
 exacerbated 40:3  
 exactly 28:22  
 example 40:6; 47:19;  
 57:10; 85:2  
 examples 55:12  
 exceed 38:16  
 except 36:7  
 exceptions 59:8  
 exchange 62:21  
 exclusively 86:8  
 Excuse 31:14,15; 62:5;  
 64:4; 88:7  
 execute 78:19  
 Executive 2:10; 4:2; 5:19;  
 10:17; 63:15; 77:22  
 exempt 62:8  
 exemption 63:24  
 Exhibits 1:2  
 exist 12:23; 17:16; 26:7;  
 63:16  
 existence 18:3  
 existing 21:16; 24:8;  
 76:21; 77:4; 82:17  
 exists 24:7  
 expect 41:7  
 expend 37:22  
 expending 83:9  
 expenditures 63:4  
 expense 59:11; 67:9;  
 71:12  
 expensive 14:3; 57:7;  
 63:10; 86:3  
 experience 35:23; 41:21;  
 43:5; 53:12  
 Expires 92:21  
 explain 72:6,7  
 explicit 23:21; 30:12; 59:8  
 express 33:4,21; 43:22;  
 45:3  
 expressed 33:11,13,17;  
 34:13  
 expressly 35:12; 38:18,24  
 extend 7:23; 8:17,24;  
 60:16  
 extended 7:1,6; 16:17;  
 45:9,11  
 extension 32:7; 35:9;  
 62:11,12; 71:4,17; 72:21,21  
 extensive 83:18; 89:14  
 extent 14:4; 35:24; 84:3  
 extra-territorial 33:17  
 extraordinarily 14:3  
 extremely 23:14; 84:15

**F**

F- 44:20  
 face 65:6,8,14; 79:20  
 facing 50:6  
 fact 13:6; 14:8; 17:21;  
 36:22; 38:15; 58:6; 71:9  
 factors 17:14; 19:12;  
 22:22; 59:4  
 fail 12:22  
 failed 34:19  
 fairly 19:11; 65:1  
 faith 23:2  
 Fall 54:2; 73:21; 86:8  
 familiar 72:4  
 family 53:8

FAQs 18:11; 22:23  
 far 14:13; 27:1; 28:22;  
 37:12,14; 41:5; 49:11; 55:7  
 favor 68:13  
 FDA 20:8; 22:8  
 feasible 14:4  
 features 89:22,23  
 February 92:18  
 Federal 24:8; 25:23,24;  
 26:16; 28:24; 32:14; 35:24;  
 36:13; 38:18; 42:1; 43:23;  
 62:12; 71:24; 72:9; 86:10  
 Federation 5:14  
 Feds 20:7,23; 26:1  
 feel 48:13; 49:6,16; 67:2;  
 68:16; 78:1  
 felt 21:3; 73:22  
 few 40:11  
 fewer 46:23; 53:9; 56:2;  
 60:17  
 field 16:23; 75:12,13  
 figure 56:24  
 file 56:16,21; 57:17  
 filed 6:11; 34:6  
 files 12:8; 57:15  
 fill 62:18; 68:17  
 final 41:18; 75:21  
 finally 29:16; 89:8; 90:15  
 financial 45:6; 47:1;  
 50:5,7; 54:7,15; 58:10;  
 65:21; 74:17; 78:16; 82:22;  
 83:1  
 find 27:7; 36:20; 63:19;  
 90:22  
 fined 59:13  
 fire 69:13  
 firm 53:3,10,13; 56:20  
 firm's 53:6  
 firms 16:11; 57:4,4,5  
 first 10:7,12; 11:17; 12:7;  
 14:14; 18:12; 23:18;  
 33:11,13; 35:10; 38:15;  
 43:1; 54:3; 55:6,15; 65:1,8;  
 71:1,9; 74:10; 82:11  
 fiscal 41:2,5,16; 63:13  
 five 46:23  
 Flag 25:13,16; 26:6; 36:13;  
 83:9  
 flawed 13:8  
 flexibility 38:20; 42:2;  
 47:9; 75:9  
 flexible 47:5; 65:2  
 Floor 1:15; 8:8  
 Floreen 5:7  
 flows 36:18  
 focused 35:8  
 focusing 76:7  
 Foley 2:18; 4:17;  
 44:15,17,20  
 folk 65:16  
 folks 21:3; 51:12; 69:20;  
 89:15  
 follow 10:6  
 follow-up 34:5  
 following 77:10  
 follows 7:12  
 for-profit 54:11  
 force 22:19  
 foregoing 92:6  
 form 43:16; 55:13  
 formal 85:10  
 formed 21:5

formerly 10:19  
 forming 10:21  
 forth 48:4  
 forward 13:13; 14:7;  
 21:12; 23:23; 27:19; 30:19;  
 41:14; 50:21; 52:13,16;  
 68:20; 71:1,22; 73:2; 80:16  
 found 46:16,18; 67:14;  
 86:12,16  
 four 12:2; 17:22; 21:7;  
 54:4; 82:8  
 Fourth 14:1; 39:21; 85:22  
 frame 29:15,20; 38:9;  
 87:4; 89:7  
 Francis 5:21  
 fraud 58:20; 67:21; 71:11  
 free 39:2; 66:14  
 freezes 83:4  
 frequently 16:23  
 Friday 1:16; 8:7; 92:8  
 front 69:18; 76:2  
 fruitful 35:3  
 FTC 37:10; 83:8  
 FTC's 25:13; 36:23;  
 37:2,7,10,14  
 full 47:24  
 fully 25:3; 36:2; 45:12;  
 48:14  
 functions 88:16  
 Fund 31:4,7,14,16,18;  
 32:4; 33:21; 37:1  
 fund's 32:15  
 fundamental 68:9  
 Funds 32:10; 34:7,23;  
 36:1; 40:1; 63:3,16,23;  
 74:19  
 Funds' 38:1  
 FURPUR 83:8  
 further 16:17; 52:1;  
 72:21; 74:8; 83:12,13  
 furthers 80:19  
 future 13:9; 21:12;  
 50:14,21

**G**

GAL 86:17  
 Gander 29:7  
 gave 22:11  
 General 1:12; 4:18;  
 6:8,21; 7:1,14,18; 11:5;  
 29:23; 30:1,13; 45:18;  
 50:10; 75:19  
 Gerry 3:11; 87:16,19,21;  
 88:14  
 gets 42:11  
 getting 43:5; 60:5; 66:18;  
 67:3; 68:1; 85:19  
 gives 22:17  
 giving 20:2; 23:20  
 GLB 72:8  
 Globe 7:10; 49:23  
 goal 11:12,15; 74:1; 86:18;  
 90:5  
 goals 44:9; 80:19; 81:23;  
 85:11,12; 88:20  
 going 11:18; 16:20; 18:20;  
 19:7,15; 22:2; 23:23; 24:7;  
 27:19; 28:8,14; 30:9,19;  
 51:12; 52:13; 55:10,11;  
 59:24; 67:4; 68:1; 69:16;  
 85:7,15

going-forward 28:16;  
 75:3; 77:20; 78:1  
 gone 14:7  
 Good 10:16; 23:2,11;  
 26:17; 29:5,6,7,11; 44:19;  
 51:16; 52:24; 61:7; 73:8;  
 81:5,6  
 goods 25:21  
 Goose 29:6  
 gotten 42:14  
 governed 78:2  
 Government 2:21;  
 4:18,21; 20:6; 28:20,24,24;  
 29:4,10,14; 44:21; 62:12;  
 81:11  
 Governor 81:23; 87:1  
 Graham-Leach 26:7  
 granted 3:22; 7:15  
 Great 3:8; 38:4; 48:12;  
 52:6; 61:20  
 Greater 4:26; 73:7,10  
 grief 65:21  
 grossly 56:7  
 Group 16:5,10,13; 21:6;  
 52:6,8; 85:10,10  
 groups 21:18; 64:20  
 growing 80:20  
 guarantying 76:12  
 guess 24:4; 90:15  
 guidance 18:10,15; 19:1;  
 21:3; 22:24; 59:6,8  
 guide 43:19  
 guidelines 21:9;  
 22:8,15,21; 36:14; 65:5

**H**

H-A-M-M-O-N 87:21  
 half 24:22; 31:13  
 Hall 64:5  
 Hammon 3:11;  
 87:16,19,21; 88:14  
 hand 19:20; 85:16; 92:18  
 handle 21:2  
 hands 21:21; 25:11  
 happen 60:11; 68:23;  
 69:13  
 happening 26:24  
 happy 73:1  
 harassment 21:2;  
 55:22,24  
 harbor 72:13  
 hard 38:5; 63:18; 65:6;  
 70:19  
 hardware 12:17; 86:3  
 harm 53:23  
 harmed 60:9  
 hasn't 24:13  
 haste 43:6  
 haven't 63:1; 91:5  
 Health 5:10; 63:15  
 Healthcare 24:15,16,21  
 hear 13:19; 15:10; 16:14;  
 19:7  
 heard 22:7; 39:12; 41:20;  
 53:15; 58:2; 82:4; 91:5  
 HEARING 1:6,8; 2:2,9;  
 3:20; 6:3,5,9,10,20,22;  
 7:8,11,21; 8:6,12; 9:6,20;  
 10:1; 11:3; 15:14,17,20;  
 17:24; 20:11,15; 22:1; 23:5;  
 30:21; 35:7; 38:7,8;

41:10,19; 43:1; 44:11,15;  
50:22; 52:19; 59:16,21;  
61:5,9; 64:2,7; 69:23;  
70:2,5; 71:17,22; 73:3;  
81:3,6; 87:12; 88:12;  
91:2,8; 92:6,9,13,16  
**heed** 43:17  
**held** 6:20; 44:2; 47:20;  
59:13  
**help** 18:22; 20:3,20,21;  
50:2,2,3; 83:2; 90:8  
**helped** 21:8  
**hereby** 92:6  
**hereunto** 92:17  
**Hi** 50:24  
**High** 5:5; 10:22,23; 55:8  
**Higher** 83:7  
**highlight** 40:11; 82:8  
**hire** 49:24  
**hiring** 83:4  
**HIRSCH** 2:24; 52:23; 53:3  
**history** 34:21  
**hold** 7:20; 46:9  
**Homeless** 62:2  
**hope** 9:23; 30:18  
**hopefully** 23:24  
**hour** 67:20; 68:2  
**hours** 12:5  
**households** 31:13  
**however** 16:12; 37:9;  
38:5; 42:5; 45:24; 74:6;  
78:12; 82:3; 88:5  
**huge** 84:19; 85:5  
**Human** 57:1; 61:13,17;  
63:15  
**hundred** 17:18  
**hundreds** 56:22; 76:19;  
83:21  
**Hunter-type** 30:7  
**hurdles** 79:19  
**Hurst** 2:14; 4:13;  
23:6,7,9,12; 87:7

**I**

**I'll** 13:19; 23:14; 51:1;  
65:15,17; 68:5; 69:20; 70:4;  
87:16  
**I've** 48:13  
**ID** 11:11; 14:11; 48:23;  
85:3  
**idea** 29:5,11; 36:16;  
67:19,21,22; 69:4  
**ideally** 25:22  
**identified** 34:17  
**identify** 49:20  
**identifying** 34:7; 85:11  
**identity** 22:9; 46:2; 58:21;  
60:10; 74:20  
**image** 32:15  
**imagine** 25:14  
**immensely** 76:22  
**impact** 33:18; 40:23;  
41:3,6; 45:6; 46:19; 80:7  
**impacted** 14:16; 73:13  
**impacting** 74:3  
**impacts** 52:12; 80:14  
**impede** 39:1  
**impermissibly** 39:9  
**implement** 19:1; 22:21;  
23:2; 24:22; 36:2,12,13;  
39:24; 40:9; 42:4; 53:13;

56:10; 57:7; 76:6; 86:19;  
87:10; 89:13; 90:8,9  
**implementation** 14:17;  
42:2,21; 47:12,24; 48:17;  
50:14; 64:23; 74:5; 80:18  
**implemented** 36:1; 60:1  
**Implementing** 14:11;  
26:14; 35:24; 37:18;  
40:2,24; 41:8,13; 79:16;  
86:7; 89:3  
**implication** 18:1  
**import** 21:13  
**importance** 32:3  
**important** 11:4; 32:17;  
45:22; 49:2; 55:4; 59:11;  
71:2; 73:18; 85:20; 87:2  
**Importantly** 31:21  
**impose** 54:24; 79:1; 82:12  
**imposed** 32:14; 46:3,11;  
83:11  
**imposing** 50:7  
**impossible** 16:16; 82:7;  
84:10  
**impractical** 13:24; 34:24  
**impression** 71:1  
**improve** 15:1  
**improved** 12:3  
**improvements** 15:9  
**improving** 11:24  
**in-elastic** 63:8  
**inability** 40:4  
**inappropriate** 47:11  
**Inc** 3:6; 4:24; 70:9  
**incentive** 72:15  
**incidentally** 57:5  
**include** 38:14; 40:15;  
55:16  
**included** 51:19; 83:17  
**includes** 51:18  
**including** 12:16; 14:15;  
20:8; 34:8; 37:1; 42:20;  
53:7; 59:9; 82:21; 83:7  
**inconsequential** 54:24  
**incorporated** 19:12  
**incorporating** 43:19  
**incorrectly** 12:15  
**increase** 63:2  
**incremental** 82:14  
**incur** 41:12; 59:11; 82:14  
**Indeed** 41:9; 54:1; 55:24  
**Independent** 5:1,14;  
44:22; 45:2,23; 46:20;  
61:19; 81:12,15  
**indicated** 36:10; 41:10;  
43:4; 46:15; 48:13  
**indirectly** 92:16  
**individual** 18:15; 20:2,19;  
53:21  
**individual's** 46:4  
**individuals** 12:19; 13:4;  
25:2; 27:2; 54:12; 62:14;  
79:14,23  
**industrialized** 13:5  
**Industries** 2:22; 4:19;  
51:5,7; 68:18; 74:15  
**industry** 14:9; 15:1;  
18:4,14; 31:7,18,20,24;  
32:4,16; 44:7; 54:15; 66:1;  
68:7; 78:24; 80:8  
**industry's** 14:8; 32:5  
**inexpensive** 68:10  
**inexplicably** 51:21

**infeasible** 12:11  
**infested** 60:6  
**influencing** 54:18  
**info** 12:13  
**inform** 91:1  
**Information** 1:10; 3:18;  
4:5; 11:11; 12:9,20; 19:7;  
22:13; 23:21; 25:22;  
32:12,19,23; 38:23; 39:3,15;  
44:2; 45:21; 46:5,13; 52:1;  
53:16,17; 54:20;  
55:14,16,19; 57:6,7,9,18;  
58:13,15; 60:9,15,18,23;  
61:2; 62:21; 65:4; 68:8,8,9;  
74:11; 76:13; 78:20,23;  
79:2; 80:20; 82:2; 83:23;  
84:2,21,24; 86:23; 87:22,24;  
88:23  
**initial** 52:15  
**inked** 77:16  
**inoperable** 13:1  
**input** 13:10  
**inserting** 78:5  
**insist** 76:11  
**instance** 19:2; 30:6  
**instances** 45:10; 71:10  
**instead** 60:5  
**Institute** 2:17; 4:14;  
31:2,5,6,8; 33:11  
**Institute's** 32:1  
**instituted** 83:4  
**institution** 82:13; 88:5,15  
**institutions** 81:16,18,19;  
83:3; 84:10,11,15; 86:22;  
88:18  
**instructive** 41:19  
**Insurance** 2:19; 4:16;  
5:15,24; 44:18,22; 45:2;  
49:1; 69:8,11,13,15,16  
**Insurers** 5:20  
**integrity** 32:12,18  
**intended** 17:4; 36:11;  
44:10; 72:12  
**intent** 30:3; 46:8; 75:15;  
78:11; 80:2; 86:1  
**intention** 39:14  
**inter-operable** 13:2  
**interacts** 16:23  
**intercepted** 58:17  
**interest** 32:15; 44:1  
**interested** 8:12; 9:4;  
92:15  
**interesting** 86:9  
**interests** 81:14  
**internal** 13:22  
**internal/external** 13:22  
**International** 16:10; 44:1  
**Internationally** 31:9  
**Internet** 3:4; 64:11,16  
**interrupted** 59:19  
**Interstate** 25:21; 39:1  
**intricately** 72:3  
**introducing** 10:4  
**inventory** 14:1; 49:15;  
68:8; 75:22; 84:18; 85:5  
**Investment** 2:17; 4:14;  
31:2,5,18; 75:3; 86:2  
**investments** 27:20; 74:4  
**investor** 32:16  
**involve** 76:1  
**involved** 92:16  
**involves** 43:5

**involving** 54:14  
**ironically** 39:24  
**issue** 11:4,21; 13:16;  
19:14; 29:20; 35:10; 48:20;  
65:20; 66:7; 71:6,23; 73:19;  
75:1  
**issued** 18:18; 33:9; 40:13;  
54:2; 55:7  
**issues** 13:15; 18:13,14;  
20:18; 21:1; 27:1; 34:7,18;  
38:14,14; 40:5,21; 48:6,9;  
52:3; 65:10; 66:10,13;  
68:19; 90:16  
**issuing** 14:14  
**ITAA** 10:20  
**ITAA)** 4:3  
**items** 79:17,24  
**its** 18:4; 32:15; 35:14,19;  
37:7,13; 41:4; 43:19; 47:10;  
49:12; 73:12,18; 76:16;  
80:3,23; 86:22  
**itself** 24:24; 53:10

**J**

**Jack** 3:3; 64:3,8,10,12  
**January** 1:16; 4:6; 5:3;  
7:2,6,7; 8:7,18; 9:10; 10:20;  
17:23; 19:16,21; 33:14;  
36:9; 38:12,13; 45:10;  
71:23; 84:9; 92:8  
**Jersey** 14:10; 24:1; 41:23;  
42:6,7,11,14,19; 47:19  
**Jersey's** 41:21; 43:4,18  
**job** 14:19; 22:20; 26:17;  
80:9; 86:6  
**jobs** 74:4  
**Johnson** 2:10; 4:2;  
10:12,14,17; 15:16,18  
**joined** 32:2  
**Joint** 4:9; 21:6; 34:1;  
36:18  
**Jon** 2:14; 4:13;  
23:6,6,7,9,12; 87:7  
**Jr** 2:18; 44:17  
**Jr.** 4:17  
**jurisdictions** 43:11

**K**

**keep** 27:3; 55:17; 76:6;  
85:17  
**key** 40:16; 67:3; 85:11;  
89:15  
**kind** 21:14  
**knowing** 40:7  
**knowledge** 84:14; 92:11  
**knowledgeable** 23:16  
**knows** 9:23

**L**

**Labor** 53:2  
**lack** 65:8; 80:12  
**lacks** 47:8  
**language** 43:23; 49:9;  
76:12; 78:6,12; 81:2  
**laptops** 8:23; 12:13  
**large** 16:11; 30:10; 31:22;  
53:18; 57:15; 66:11,22;  
88:5,15,16  
**largely** 35:3

larger 28:1; 60:23; 76:18  
 largest 10:22; 41:12  
 last 6:13; 10:3; 17:23;  
 34:16; 40:13; 54:2; 64:14;  
 70:10; 71:22; 73:21; 79:9;  
 86:11,17  
 lastly 79:9  
 later 19:19; 59:14  
 latitude 75:18  
 Law 16:10,11;  
 24:8,12,13,15,16,21,23;  
 26:16; 29:23; 30:2; 32:14;  
 38:18; 39:17; 42:1; 43:23;  
 47:6; 48:23; 49:11;  
 53:2,10,13; 54:4; 56:2,20;  
 57:4; 65:1; 67:23; 72:12  
 Laws 1:12; 6:21; 7:14,18;  
 26:18; 49:4; 55:22  
 layoffs 55:3  
 lead 53:22; 64:22; 66:3;  
 69:1  
 leadership 65:20  
 leading 12:5; 66:2; 69:1  
 leads 53:19  
 League 3:6; 4:24; 70:9,14  
 lean 84:11; 86:6; 90:19  
 learned 60:21  
 learning 56:20  
 least 13:10; 19:12; 29:15;  
 31:13; 60:16,19; 64:22  
 leave 30:17; 57:2  
 leaves 13:9  
 leaving 58:16  
 Lefkowitz 16:5  
 legal 46:2  
 legislating 65:9  
 legislation 11:14; 14:12;  
 69:5  
 Legislative 41:10; 62:18;  
 86:1  
 Legislator's 46:7  
 Legislature 11:5; 30:4;  
 44:10; 63:2; 68:22  
 Legislature's 34:1; 46:7  
 legitimate 19:10  
 length 17:8  
 lengthy 34:6  
 lens 80:11  
 less 37:14; 39:24; 49:24  
 let's 10:9; 19:21; 26:2;  
 27:7,15; 28:12,12,16,17  
 Letter 4:6,22; 5:1,9,15,20;  
 15:19; 23:18; 33:16;  
 34:6,16,18; 37:17; 40:22;  
 43:7; 47:22; 48:4,7; 51:23;  
 65:23  
 letterhead 4:6,22;  
 5:1,9,15,20  
 letters 18:18; 30:10  
 level 22:23; 25:23; 53:23  
 level-funded 62:24  
 level-funding 63:8  
 levels 20:7  
 liable 59:14; 69:10  
 Liberal 88:1  
 library 18:21  
 Licensing 63:5  
 Licensure 4:10; 34:2  
 lieu 43:8  
 Life 5:15  
 light 36:21; 43:15  
 limit 55:3

limited 27:1  
 limiting 79:4  
 limits 79:1  
 Lindsey 1:12; 92:4,20  
 line 14:5; 24:4; 58:19  
 link 37:7  
 linked 36:17  
 list 10:12; 65:5; 91:3  
 listed 89:23  
 listen 51:13,22  
 listened 42:6  
 listening 14:7; 42:13;  
 43:1  
 Lists 26:13  
 litany 68:19  
 literally 24:21  
 litigate 59:12  
 Litigation 53:2; 57:11  
 little 65:12; 84:13  
 lives 68:7  
 LLP 2:13; 16:2  
 located 76:24  
 lock 57:2  
 lockable 56:16  
 locks 56:16,22  
 long 14:17; 26:12; 32:10;  
 75:16; 76:15  
 longer 60:19  
 Longhorn 60:4  
 longstanding 79:3  
 look 14:17; 24:6; 26:6;  
 28:12; 41:14; 50:21; 52:16;  
 64:19; 65:13; 71:8; 72:12  
 looking 24:5,5; 58:12,18;  
 72:21  
 looks 80:16  
 loss 37:5; 49:21; 65:21;  
 76:7; 80:10  
 losses 69:11  
 lost 56:8,9  
 lot 11:19; 13:19; 18:8,8;  
 19:8; 21:24; 23:15; 24:24;  
 25:1; 27:24; 28:7; 65:11,13;  
 66:6,24; 67:1,4,6; 68:4;  
 69:8; 82:4; 85:15; 89:2;  
 90:20  
 lots 22:17  
 love 13:15  
 low 55:7

**M**

M.D. 5:11  
 M.G.L 3:21,25  
 MA 1:16,21; 2:5  
 MacDougall 2:20; 4:20;  
 50:23; 51:1,4,6; 59:15,23  
 machines 66:17  
 MAIA 45:22; 48:24  
 mail 58:17  
 mailed 9:12  
 maintain 54:20; 57:24;  
 60:18  
 maintenance 55:6  
 major 14:18; 48:11  
 make 17:10; 23:2; 25:2;  
 26:2,8,17; 27:2,19; 29:14;  
 42:11; 67:24; 68:23; 77:10;  
 91:4  
 makes 39:23; 48:5; 84:13  
 making 11:24; 14:20;  
 17:13

manage 31:9  
 managed 22:14  
 Management 87:24  
 Manager 5:22  
 managing 31:19  
 mandate 46:8; 49:12;  
 82:12,19; 85:24  
 mandated 58:1  
 mandates 62:18  
 Mandatory 24:16; 49:11  
 manner 33:5  
 manuals 22:11  
 Mark 2:12; 15:22,23;  
 16:1,3; 20:15; 68:3  
 market 77:2  
 Marketer 26:20  
 marketing 79:4  
 marketplace 69:19  
 marriage 92:14  
 Mary 3:5; 4:25; 69:24;  
 70:1,4,8,10,11  
 Marylou 5:11  
 Mass 7:14; 11:2; 20:24;  
 21:6; 67:20; 68:2  
**MASSACHUSETTS**  
 1:4,12,14; 2:15,19,22; 3:6;  
 4:12,16,19,24; 5:2,5,8,9,16;  
 7:9; 13:5; 14:5; 17:19;  
 20:8; 21:5,18; 23:10,13;  
 24:3,13; 25:17; 26:13;  
 28:11; 30:9; 31:17,18;  
 36:23; 39:17; 41:23;  
 42:5,24; 43:9; 44:18,22;  
 46:12,13,20; 47:16,23; 50:1;  
 51:5,7; 54:14; 59:23;  
 61:13,17; 66:21; 70:9,13;  
 76:24; 81:13,16,18; 88:2;  
 92:2,5  
 Massachusetts' 37:1  
 massive 84:8  
 matches 69:17  
 matter 11:7; 32:9; 41:18;  
 66:14; 92:16  
 Matters 16:9  
 mature 67:7  
 May 7:3; 9:1,11; 16:17,21;  
 17:4,11; 19:16,18,23;  
 21:15,16; 22:19; 25:18;  
 27:24; 32:20; 36:6,11,14;  
 37:23,23; 38:12; 45:9; 47:3;  
 48:14; 56:7,21; 57:23;  
 58:4,6,7,14; 65:15  
 maybe 17:18; 29:11  
 MCAD 21:4,7  
 McCarin 3:9; 5:4;  
 81:4,5,8,10,10  
 mean 17:13; 90:6  
 meaning 40:17  
 meaningful 11:14; 34:20;  
 43:20; 49:19  
 means 13:12; 92:23  
 meant 19:2  
 measure 46:19  
 measured 14:13  
 measures 52:18  
 mechanism 63:11  
 mechanisms 18:5; 63:9  
 media 12:21; 18:4  
 medium 67:1  
 meet 63:5; 82:7; 84:4;  
 85:20; 86:18  
 Meeting 22:12; 34:5;  
 84:16

meetings 18:4; 38:3  
 member 11:10; 45:7,12;  
 46:14,22; 48:2,10; 84:10;  
 86:22  
 members 12:6; 15:4,11;  
 31:4,8; 32:1,21; 33:5;  
 37:17; 39:16; 41:7; 45:22;  
 48:13,24; 51:8,10,11; 53:3;  
 62:15; 70:16,17,20; 71:13;  
 73:12,18  
 mental 62:4  
 mentioned 52:9; 89:8  
 mere 59:24  
 merged 10:20  
 merit 74:8  
 met 33:19; 35:11  
 Michael 3:1; 4:23;  
 61:6,7,12,14,14  
 Michalove 4:8,11  
 Microsoft 4:6; 15:5,19  
 mid-sized 67:5  
 miles 67:20; 68:2  
 millions 32:22; 41:7  
 minimis 41:2  
 minimizing 53:22  
 minimum 36:1  
 minute 59:17  
 missed 67:15  
 mission 71:13  
 Model 22:23  
 modifying 39:15  
 Mom-and-Pop 25:12  
 moment 20:12; 44:12  
 monetary 57:20  
 money 47:2; 55:20; 61:20;  
 63:9,19; 66:24; 69:11  
 monitory 56:8  
 months 26:15; 37:12;  
 54:3; 75:24  
 Moreover 36:24; 43:4  
 Morrissey 40:22; 43:14  
 Morrissey's 41:15; 43:7,18  
 mostly 61:19  
 movement 39:3  
 moves 68:20  
 multi-party 78:14  
 Murray 2:2; 4:8; 6:3,7;  
 15:14,17,20; 20:11,15; 22:1;  
 23:5,11; 30:21; 44:11,15,19;  
 50:22; 52:19; 59:16,21;  
 61:5,9; 64:2,7; 69:23;  
 70:1,2,5,20; 73:3,15; 80:22;  
 81:3,5,6; 87:12,17; 88:12;  
 91:2  
 Mutual 31:4,7,14,16,18;  
 32:4,10; 33:20; 34:7,23;  
 36:1; 37:1; 38:1; 40:1  
 mutually 13:1

**N**

name 6:7; 10:16; 16:3;  
 23:12; 31:3; 44:20; 51:6;  
 53:1; 61:14; 64:12,14;  
 70:11; 73:8; 81:10;  
 87:13,21  
 names 10:4  
 Nation's 10:22  
 National 5:13; 23:20;  
 31:6; 34:11; 43:24  
 nature 38:8,11; 47:10;  
 49:12; 76:3

near 43:15  
 nebulous 67:12  
 necessarily 56:18  
 necessary 11:17; 12:16; 19:9; 32:24; 47:1  
 need 18:13; 19:19,22; 20:20; 24:8; 29:10; 38:22; 52:4; 66:17,23; 78:17; 80:5; 89:18,18  
 needed 11:9; 21:3; 76:8  
 needs 18:2,24; 41:4; 46:1; 47:4,5  
 negates 49:13  
 negotiate 76:11  
 Network 3:4; 64:11,17  
 networks 12:10  
 New 2:11; 10:15,17; 13:22; 14:10; 24:1; 27:11,19; 32:5,24; 33:2; 35:13,18; 36:13; 41:21,23; 42:6,7,11,14,19; 43:4,18,22; 47:19; 54:4; 56:21; 73:24; 75:3; 77:15; 80:10,15; 82:15  
 Newbury 3:12; 87:14,20,22; 88:1  
 Next 18:24; 19:16; 27:16,17; 69:20; 75:18,22; 76:9; 78:20  
 non- 59:12  
 non-profit 53:7; 61:18  
 non-profits 24:20; 61:2  
 non-public 32:12; 44:2  
 non-workable 13:20  
 none 53:21  
 Norfolk 92:3  
 North 1:21  
 Nos 8:8  
 not- 54:10  
 not-for-profit 54:5  
 Notarial 92:18  
 Notary 1:13; 92:4,20  
 Notice 3:20; 7:8,11; 9:19  
 notifications 54:2  
 Notwithstanding 33:3; 36:4  
 November 6:13; 7:9; 8:5; 33:19,24; 34:4,5,18; 35:12  
 nowhere 62:21  
 number 11:23; 15:10; 17:15; 18:23; 19:15; 20:3,6,7; 57:13; 74:16,17; 85:3; 90:17  
 numbers 54:11; 74:14,18,19,22  
 numerous 16:14

**O**

O'Brien 5:22  
 o'clock 6:6  
 O'Connell 11:1; 40:23; 43:8; 49:22; 70:21  
 O-L-E-Y 44:21  
 object 68:14  
 objections 16:15,19  
 obligate 12:7,12  
 obligation 14:2; 32:11,13  
 obligations 7:5; 19:22  
 observations 16:22; 64:21  
 obtain 9:17; 20:21; 78:7  
 obtaining 8:19; 84:7

obviously 18:12; 48:11; 60:5  
 OCABR 73:21  
 occasional 57:8  
 occur 29:9; 58:21  
 occurred 29:3,4  
 occurs 78:16  
 October 33:16  
 of-the-art 12:17  
 offer 72:24; 73:1; 87:3  
 offered 6:23  
 offering 77:2; 87:8  
 Office 2:3; 3:23; 5:17; 6:8,12; 7:16,19; 9:12; 11:2; 14:22; 22:13; 55:6; 56:14; 57:2; 60:14; 63:15; 86:17; 92:7  
 Officer 5:19; 6:3,9; 15:14,17,20; 20:11,15; 22:1; 23:5; 30:21; 44:11,15; 50:22; 52:19; 59:16,21; 61:5,9; 64:2,7; 69:23; 70:2,5; 73:3; 81:3,6; 87:12,22; 88:12; 91:2  
 Officer/General 2:2  
 official 42:12  
 officials 10:5; 34:13; 45:19; 50:11  
 often 13:1; 55:8; 57:12; 76:11  
 Okay 15:19,20; 70:4; 87:15; 91:7  
 on-going 76:2; 79:13; 82:22  
 ONE 6:17; 15:4; 16:22; 17:15,17,18; 22:11,18; 25:19; 26:19; 29:16; 31:14; 40:21; 44:12; 48:11,11; 53:4,15; 55:9; 56:6; 58:23; 63:1,20; 65:7,17; 66:19; 68:5; 69:4; 70:17; 72:5; 77:12; 87:15; 90:18  
 one-size-fits-all 39:22; 47:9; 59:3  
 onerous 86:4,5; 89:10  
 open 13:9; 27:3; 55:2  
 Opening 2:9; 35:3  
 operate 31:8; 62:5  
 operating 12:17; 49:3; 63:3; 82:10  
 operation 80:10; 90:8  
 operational 54:23; 79:4  
 Operations 61:16  
 opportunity 8:13; 9:5; 10:24; 45:3,16; 50:20; 52:10,14; 61:8; 69:21; 73:17; 80:24; 81:20; 87:11; 90:22; 91:1  
 opposed 28:17  
 opposition 43:16  
 options 79:5,22  
 Oracle 16:6  
 oral 8:14; 9:6  
 order 46:4; 72:1; 77:10,22; 78:19; 79:24  
 order! 6:5  
 organizations 12:19; 13:4; 18:5; 23:19; 24:20; 26:9; 53:8; 61:19  
 original 17:23; 86:1  
 originally 8:1; 41:24; 47:6  
 ostensibly 35:8

others 15:1; 26:4; 39:16; 40:2; 50:17  
 otherwise 20:22; 23:1  
 ought 29:6  
 out-of-State 49:24  
 out-source 90:19  
 out-weight 58:23  
 outline 38:10  
 outreach 18:2,5; 25:1  
 outside 20:4; 39:4; 55:19; 76:24; 83:21  
 outstanding 52:4  
 over-broad 56:7  
 over-burdened 84:12; 86:6  
 over-protect 59:11  
 overall 74:4  
 overlooked 55:1  
 overly 33:22; 39:21; 41:24; 75:15; 79:1  
 oversight 56:18  
 owe 14:18  
 own 18:4; 26:8,9; 31:13; 35:19; 36:4; 41:4; 56:20; 64:14; 71:11,12  
 owned 53:8

**P**

p.m 1:17; 8:7  
 Page 2:8; 3:15,25; 49:3  
 Pages 1:1; 3:19; 57:18  
 PALMER 2:13; 16:2,4  
 paper 56:13; 57:3,3  
 paramount 62:16; 71:7  
 Park 1:16; 2:4; 8:10  
 part 11:22; 38:6; 57:12,15; 71:12; 77:15; 80:11  
 particular 13:16; 48:21; 77:2  
 particularized 20:20  
 particularly 26:23; 27:6,22; 61:1; 63:12; 67:9; 82:5,20; 84:11; 86:4,5  
 parties 8:13; 9:4; 13:19; 92:15  
 Parts 54:22; 72:14  
 party 7:6; 8:20; 27:22; 83:15  
 passed 24:16; 26:13,16; 47:6  
 past 85:18  
 Patrick 11:6; 45:13; 81:24; 87:1  
 pay 63:10  
 payments 37:3  
 payroll 27:3  
 PCI 5:21; 68:18  
 PDAs 19:4  
 peculiar 36:21  
 penalties 67:12,13  
 penalty 67:19,21; 68:1  
 penmanship 87:17  
 penny 63:1  
 people 11:20; 17:22; 23:15; 24:14; 26:3; 27:5; 28:8; 52:7; 53:4; 57:1; 60:20; 62:2,3; 64:18; 65:21; 66:8,18; 67:23; 68:3,4,6; 69:7; 86:14  
 percent 61:24  
 perfect 52:17

perhaps 16:16; 23:24; 67:14; 71:18; 77:1; 83:21  
 period 21:15,15; 37:11; 48:18; 50:15; 87:8,9  
 permanent 38:7  
 permit 37:3  
 persists 80:13  
 person 56:15  
 person's 38:20; 45:20; 46:2; 74:20  
 Personal 1:10; 3:18; 4:4; 11:11; 12:9,13; 44:2; 45:20; 46:4,12; 54:20; 55:18; 57:6,9; 58:13; 61:2; 74:11; 76:13; 78:20,22; 80:20; 82:2; 83:23; 84:2,24; 86:23  
 personally 39:12  
 personnel 47:2  
 persons 31:23; 36:12,24; 37:13; 39:3; 40:8; 42:10; 43:21; 44:3  
 perspective 27:7; 48:9  
 pertain 82:9  
 Peter 16:5  
 phased-in 48:17  
 phrase 13:10  
 physical 56:12; 62:4  
 piece 57:8,18; 58:13  
 Pike 67:20; 68:2  
 place 25:15; 48:1; 72:13; 75:7; 76:20; 84:1; 89:21  
 placeholders 23:1  
 places 60:23  
 placing 79:5  
 plaintiffs 21:9  
 plan 66:19; 80:1  
 Plans 5:10; 22:16; 76:6  
 plastic 71:10  
 Plaza 1:16; 2:4; 8:10  
 please 6:4; 10:11; 44:12; 59:18; 88:8  
 Please! 88:9  
 plight 63:14  
 point 24:11; 29:17; 47:14; 48:8; 55:21; 66:24; 86:9  
 point-of-sale 27:12  
 pointed 45:14  
 points 25:7; 65:3  
 Policies 55:17; 56:5; 89:10,12  
 Policy 22:23; 51:16; 52:18; 55:23; 56:10; 73:10; 87:3  
 poorly 68:17  
 portable 8:22; 12:14,21; 19:3; 36:7  
 portion 83:22  
 pose 53:23  
 posed 58:13,16  
 position 20:2; 51:15  
 positive 74:6  
 possesses 46:12  
 possibility 13:9  
 possible 79:22  
 Postal 1:20  
 posted 18:16  
 potential 22:4; 34:14; 49:21; 76:7  
 practically 58:12  
 practice 78:24; 87:16  
 practices 76:14  
 pre-existing 84:3

pre-proposed 14:14; 42:9,16,21  
precedence 43:6  
precedent 20:5,21  
precision 40:7  
preclude 39:2  
preferable 86:19  
preliminary 32:9  
premises 55:19  
preparing 18:21  
prescribed 63:4  
prescribing 75:10  
prescriptive 33:22; 34:24; 39:22; 41:24; 49:12; 75:15  
present 9:6; 13:24; 15:4; 23:17; 34:22; 51:22  
presented 35:22; 41:9; 79:22  
President 4:13,18,21; 5:4,7,12,18,22; 23:12; 44:21; 81:11  
press 41:1  
presumably 36:16  
pretty 23:21  
prevent 60:2; 75:11  
previous 24:10; 35:22; 38:2; 45:14  
previously 8:4; 41:20  
Primarily 62:11  
primary 78:18  
Principal 4:11  
principle 78:3  
principles 19:11; 22:22; 81:23  
prior 47:15  
Privacy 16:5,7,9; 21:17; 33:4; 41:22; 42:17; 49:3; 74:1; 76:7; 80:18  
private 11:12; 30:4,14; 35:18; 46:10  
privately 53:8  
probably 17:2,22; 18:6; 69:16  
problem 56:1; 65:18; 66:2; 68:24  
problems 53:14; 65:7; 67:8  
procedures 13:22; 22:9; 85:13,13  
process 14:16; 19:6; 23:24; 25:6,6; 26:23; 37:20; 43:6,12,12; 44:4; 47:24; 50:18; 57:13; 75:23  
processes 79:4  
product 77:2  
productivity 56:9  
products 25:21  
Professional 4:10; 34:2; 65:4,19; 66:12  
profit 64:16  
program 55:16  
programs 17:20  
prohibitive 79:18  
project 85:11  
promulgated 8:2,4  
promulgation 1:9; 7:22; 47:12  
Property 5:20  
propose 68:11  
proposed 33:14; 37:19; 41:24  
prospect 76:20

Protect 4:4; 14:21; 32:11; 52:18; 82:2; 84:2,24  
protected 46:5  
protecting 11:11; 32:15,18; 44:2; 45:20; 46:2; 80:20; 86:23  
Protection 1:10; 3:17; 4:10; 34:1; 43:12; 51:16; 71:6  
protections 43:10  
prove 76:22; 79:17  
provide 8:13; 34:21; 38:5,19; 42:2; 45:15; 54:8; 62:1; 63:11,19  
provided 37:11; 44:5; 51:24  
Provider 13:17  
providers 7:6; 8:20; 27:22; 28:2; 49:6; 57:24; 61:13,17  
Providers' 3:2; 4:22  
providing 37:13; 39:18  
provision 71:21; 77:11,18  
provisions 1:12; 7:13,24; 9:3; 34:24; 36:6; 40:15,18; 45:4,6,10; 48:19; 49:6; 71:24; 83:16; 84:1  
PUBLIC 1:6,8,13; 3:20; 6:10,20; 7:8,11,11,21; 8:11; 9:20; 11:12; 12:10; 37:20; 42:11; 44:5; 46:9; 51:16; 52:18; 73:9; 77:21,23; 87:2,8; 89:4; 92:4,6,9,13,20  
publicize 18:2  
publicized 18:15  
published 7:9  
purchase 75:4; 82:15  
purchasing 56:21  
purpose 8:11; 71:16  
purpose? 19:10  
pursuant 1:11; 3:21; 6:20; 7:13,18; 8:21,23  
pursuing 42:12; 87:2  
push 65:11  
put 13:13; 18:11,16; 22:15; 26:3; 30:10; 48:4; 68:22,22,23  
putting 22:8; 25:15; 26:8

**Q**

question 38:9; 40:8; 51:17; 68:3  
questions 19:15; 72:24  
quick 70:4  
quickly 66:5  
quite 22:7; 90:17,23  
quote 43:11; 79:24  
quoted 49:22  
quotes 41:1,4

**R**

R-I-P-P-L-E 61:15  
radio 18:3  
raise 21:20; 28:20; 29:17; 40:20; 41:18  
raised 40:5,14,22; 48:7  
ramifications 25:4  
random 58:13  
range 66:16; 84:14  
ranges 62:4

rapidly 75:12  
Rather 55:10; 59:12; 79:23  
re-negotiation 13:21  
re-promulgation 43:21  
reached 72:3  
reaction 90:3  
read 5:4; 65:3; 87:13  
readily 12:18; 13:3  
reading 65:1  
reads 7:11  
ready 44:8; 52:7; 89:14  
real 13:24; 18:24; 19:20; 26:5; 27:1; 28:22; 59:6  
reality 26:24; 29:1; 59:7  
realize 58:22  
reallocate 82:16  
really 11:17; 14:17; 24:4,15,18; 25:3,17; 26:18; 27:8,15,24; 28:5,8,23; 29:22; 30:10; 58:15; 64:12; 65:13; 69:5; 71:17,20; 79:12; 90:7,24  
reams 57:6  
reason 32:21; 62:23; 72:19  
reasonable 9:5; 27:7; 35:19; 46:1; 87:4  
reasonableness 49:13  
reasonably 12:19; 19:9  
reasons 60:12; 62:10; 71:20  
reassess 29:10  
Reauthorization 83:7  
recap 33:13  
receipt 36:8; 58:16  
receive 61:20,23  
received 35:16  
receiving 39:14  
recent 32:6; 35:8; 40:22; 41:21; 43:7; 46:18  
recently 22:7; 49:22  
recognize 11:13; 12:22  
recognized 47:20  
recommend 43:17; 74:20; 75:2  
recommendation 49:8,18  
recommendations 25:19; 48:4; 87:7  
recommended 47:21  
reconsider 60:14  
reconsideration 24:6  
record 5:4; 38:7,11; 44:14,20; 70:11; 92:12  
record.] 9:21  
records 12:8; 55:18; 56:13; 84:19; 85:6,16; 89:17  
record] 6:19; 20:14; 44:13  
Red 25:13,16; 26:6; 36:13; 83:8  
reduced 82:23  
redundant 46:9  
reevaluate 60:24  
refine 85:13  
reflect 80:2  
reflects 17:24; 36:16  
Reg 18:7  
regard 47:10; 55:4; 80:24  
regarding 8:14; 34:2,22; 39:18; 41:2; 49:3; 87:7  
regardless 32:19

regards 31:12  
Regional 5:22  
Register 7:9  
Regs 16:20; 17:1,7,7,19; 18:3; 19:1; 22:14,19,21; 72:10,20  
regulate 41:22  
regulated 42:14; 45:18; 47:17; 50:10  
REGULATION 1:5; 2:3; 3:24; 5:18; 6:9,15,18; 7:17,20; 13:18; 14:23; 23:22; 25:23; 28:11,16,23; 29:19; 33:7; 45:5,9,11,21; 47:8; 49:16; 54:1; 71:22; 72:2; 74:3,8,13,17,21,23; 75:5,21; 78:13; 79:8,16; 80:3,11,19; 92:7  
Regulation's 45:6  
regulations 8:1,3,5; 9:14; 11:3,14; 12:3,15,22; 13:8; 14:6,11,15,20; 16:15; 17:3,11,14,16; 21:11; 23:3; 25:8; 27:14; 38:10; 42:9,15,20; 45:17; 46:7; 47:3,13; 48:1,12,23; 51:19; 52:12; 53:14; 54:22; 55:12,15; 56:11,21; 57:15,22; 58:24; 59:2; 60:3,15,24; 62:8,13,17; 63:10,23; 65:5; 71:1,5; 73:13; 77:9; 80:7; 81:21; 82:5,6,11,18; 83:11,13,17; 84:5,14,20; 85:7; 86:19; 88:21; 89:4,23  
Regulator 72:9  
Regulatory 36:17,22; 39:10; 54:18; 59:10  
reinventing 43:9  
reissuance 87:9  
reissue 50:11,13; 71:10  
reiterate 16:18; 35:5  
reiterated 72:8  
relate 6:23; 83:22  
related 53:5; 71:17; 72:19  
relates 40:23  
relating 40:16  
Relations 81:11  
relationship 70:18  
relative 48:5,16  
reliable 67:7  
rely 90:19  
remain 40:15; 80:14  
remains 31:17  
Remediation 22:16  
removal 77:6,8  
remove 74:21  
removed 79:8  
renegotiate 28:10; 58:5; 76:21  
renegotiated 84:5  
reopen 76:20  
replace 27:17  
Report 54:1,13  
reported 54:3  
Reporter 1:13; 44:12; 64:4; 88:7; 92:5,24  
reporting 59:24  
represent 42:16; 46:17; 51:6; 58:4; 60:13  
representatives 14:15; 33:20  
representing 10:23; 31:4;

<p>51:8; 61:18  <b>represents</b> 45:1; 81:14  <b>REPRODUCTION</b> 92:23  <b>reputation</b> 76:15  <b>request</b> 34:4; 41:15; 66:4; 90:1  <b>require</b> 27:8,8; 28:14; 39:19; 54:22; 55:15,22; 56:11,21; 57:16,22,23; 63:21; 78:6,13; 79:24; 83:11; 86:2; 89:14  <b>required</b> 38:18,24; 75:2; 82:16,24; 85:17  <b>requirement</b> 14:1; 49:15; 76:22; 77:4,7,8; 84:18; 85:23; 89:24  <b>requirements</b> 7:4; 32:14; 33:22; 34:9; 36:3; 37:23; 39:6,10; 46:3; 47:2; 56:17; 59:3; 60:1; 73:24; 74:7; 80:15; 83:6; 84:4  <b>requires</b> 13:21; 48:23; 88:17  <b>requiring</b> 28:12; 29:9; 56:6; 77:14,19; 83:18  <b>Research</b> 54:9  <b>Resi-</b> 3:18  <b>reside</b> 32:20  <b>resident</b> 46:13  <b>Residents</b> 1:10; 54:15; 63:20; 81:19  <b>resource</b> 22:5; 57:1; 79:18; 80:5  <b>resources</b> 21:16; 27:1; 37:22; 38:22; 47:1,5,10; 76:7; 82:17; 83:1,10,18; 89:14  <b>respect</b> 9:2; 19:14; 48:22; 71:4  <b>respectfully</b> 35:20; 42:23; 72:24  <b>respond</b> 25:14  <b>responders</b> 71:10  <b>response</b> 19:24; 20:18; 35:16; 37:20; 41:15  <b>Response]</b> 10:8; 91:6  <b>responsibilities</b> 25:4  <b>responsibility</b> 17:10  <b>responsiveness</b> 79:13  <b>restaurant</b> 58:17  <b>restaurants</b> 25:12  <b>restraint</b> 80:9  <b>restricted</b> 82:24  <b>restrictions</b> 56:12; 57:8  <b>restrictive</b> 79:1  <b>result</b> 7:2; 63:7; 82:14  <b>results</b> 12:4  <b>retailer</b> 27:11  <b>Retailers</b> 2:15; 4:12; 23:10,13; 24:3; 25:10  <b>retained</b> 79:3  <b>retention</b> 78:22  <b>retroactively</b> 75:7  <b>retroactivity</b> 75:1; 77:13  <b>return</b> 57:14  <b>revenue</b> 80:9; 82:24  <b>review</b> 12:5; 50:11,13; 64:23  <b>revise</b> 32:24  <b>revised</b> 42:8,9,15  <b>revising</b> 74:21  <b>revision</b> 80:2</p>	<p><b>revisions</b> 77:10  <b>revisit</b> 13:16  <b>Richard</b> 5:3  <b>rid</b> 60:5  <b>right</b> 15:2,12; 23:20; 24:10; 25:11; 29:5; 30:4,14; 42:11,14,20,24; 43:5; 67:4; 68:24; 69:1; 70:5; 83:6; 85:19; 88:10  <b>rigorous</b> 41:5; 45:15  <b>Ripple</b> 3:1; 4:23; 61:6,7,12,14,14  <b>risk</b> 30:11; 49:20; 58:12,16; 59:13; 67:23; 69:7,12  <b>risk-based</b> 76:5  <b>risks</b> 53:24; 58:23  <b>road</b> 65:24  <b>Robert</b> 3:9; 5:4; 81:5,8,10,10  <b>ROBERTS</b> 2:24; 52:23; 53:3  <b>robust</b> 17:3  <b>Rogers</b> 72:2  <b>role</b> 11:13; 65:20  <b>Room</b> 1:15; 8:8; 11:8; 17:21; 52:7  <b>routinely</b> 47:16; 78:15  <b>Rule</b> 37:10,23; 40:16; 41:20; 72:14  <b>rulemaking</b> 33:7  <b>Rules</b> 25:14,16; 26:6,6; 33:8,14,22; 34:3; 35:6,24; 36:12,23,23; 37:1,2,7,13,14,15,18; 38:15,19; 39:1,8,21; 40:2,5,8,12; 41:8,13,21; 42:1,16; 43:16,20,21,22; 44:6,9; 46:9; 48:17; 50:13; 83:9  <b>Rules'</b> 41:17  <b>run</b> 65:10,10  <b>running</b> 88:10  <b>rush</b> 68:16</p> <p><b>S</b></p> <p><b>S-C-H-R-E-I-</b> 16:3  <b>S-W-E-E-N-E-Y</b> 73:9  <b>safe</b> 72:13  <b>safeguards</b> 58:1  <b>safety</b> 76:12  <b>salary</b> 55:9  <b>Salmon</b> 2:16; 4:15; 30:22,23; 31:1,3  <b>satisfy</b> 76:21  <b>saying</b> 64:24  <b>says</b> 50:5  <b>scalability</b> 80:4  <b>scarce</b> 82:17; 83:1  <b>schedule</b> 18:4  <b>scheme</b> 54:19  <b>schemes</b> 59:10  <b>school</b> 85:2; 86:8  <b>schools</b> 82:24; 83:6; 85:9,16,23; 86:5  <b>Schreiber</b> 2:12; 15:23; 16:1,3; 20:13,16; 22:4  <b>Schrieber</b> 15:22  <b>Scientific</b> 54:9  <b>scope</b> 18:7; 38:21; 59:4; 80:4; 84:20</p>	<p><b>scratch</b> 28:18  <b>Seal</b> 92:18  <b>seamless</b> 43:11  <b>seat</b> 70:3,6  <b>SEC</b> 26:7  <b>Second</b> 1:15; 8:8; 13:7; 18:10; 19:9; 39:1; 56:11; 62:23; 74:24; 83:14  <b>secondly</b> 75:9  <b>seconds</b> 66:14  <b>Secretary</b> 6:12; 11:1; 40:23; 43:8; 49:22; 70:21  <b>Section</b> 12:7; 13:8,18; 14:2; 72:11  <b>sector</b> 35:18; 46:10; 51:8; 54:7; 62:7,23; 63:14  <b>sectors</b> 11:12; 82:20  <b>secure</b> 13:11,12; 19:23; 57:16,16; 69:12  <b>securing</b> 76:15  <b>Security</b> 3:4; 4:11; 22:16; 32:5,18,23; 33:2; 38:23; 39:23; 41:22; 42:18,20; 46:5; 48:3; 49:4; 53:19; 55:16,17; 57:13; 64:11,16,17; 65:4; 68:8,9; 74:16; 76:12; 80:6; 85:3; 88:22; 89:3,10  <b>seeing</b> 41:14  <b>seek</b> 63:23  <b>seeking</b> 60:2; 73:23  <b>seemingly</b> 57:16  <b>seems</b> 56:15; 65:1; 85:20; 89:10  <b>seen</b> 24:1  <b>segregate</b> 57:17  <b>sell</b> 66:21  <b>seminars</b> 89:4  <b>Senator</b> 40:22; 41:15; 43:7,13,17  <b>Senior</b> 5:7  <b>sense</b> 65:5,9,10; 84:13  <b>sensitive</b> 11:11  <b>sent</b> 34:17  <b>sequentially</b> 85:12  <b>series</b> 72:10  <b>serious</b> 33:5,21; 34:13,23; 41:10,16; 45:4; 56:1  <b>seriously</b> 32:10; 45:23; 89:5  <b>serve</b> 31:10; 52:8; 62:15,15; 70:13,16  <b>service</b> 7:6; 8:20; 13:17,21; 28:2; 49:6; 53:7,9; 54:7; 57:24; 61:13,17; 77:2; 79:5  <b>services</b> 25:22; 54:9,15; 62:1,3,3,15; 63:15,20; 78:16  <b>serving</b> 71:13  <b>set</b> 45:16; 50:13; 52:17; 79:22,23; 87:4; 92:17  <b>setting</b> 22:20  <b>seven</b> 46:21  <b>several</b> 16:22; 17:14; 18:18; 51:11; 52:3; 64:18; 66:20; 75:23; 84:22  <b>severe</b> 17:3  <b>sexual</b> 21:2; 55:22,24  <b>share</b> 11:13; 50:20; 64:21; 72:18; 74:2  <b>shared</b> 80:19  <b>shareholder</b> 32:20</p>	<p><b>shareholders</b> 31:11,14; 32:19  <b>shareholders'</b> 37:4  <b>sharp</b> 47:13  <b>Sheet</b> 9:24; 10:2  <b>short</b> 45:12  <b>shortly</b> 33:15  <b>Shoulder</b> 58:18  <b>Sign</b> 9:24; 10:1  <b>signed</b> 4:8; 5:3,11,18,21  <b>significant</b> 21:12; 54:23; 82:14; 83:22; 85:8  <b>significantly</b> 12:3; 52:11; 74:3; 82:23  <b>similar</b> 21:14; 25:5,8; 26:22; 27:21  <b>similarities</b> 36:22  <b>simple</b> 65:13  <b>simply</b> 22:22; 42:24; 66:8,17; 69:9; 77:3  <b>single</b> 54:17; 56:6; 57:17  <b>sister</b> 39:12  <b>sit</b> 65:15  <b>sites</b> 62:6  <b>situation</b> 63:13; 68:18; 79:21  <b>six</b> 56:2  <b>size</b> 38:21; 46:21; 59:4; 78:24; 80:4  <b>sized</b> 67:2  <b>sizes</b> 80:8  <b>skewed</b> 54:19  <b>small</b> 27:6,10,22; 28:5; 46:17; 47:5; 50:8; 53:6,10,17; 54:7,10,12,19; 55:13; 56:1,9; 58:4,7,14; 59:8; 60:8,13,15; 61:1; 66:6,7,11; 67:1,4; 79:10,14,18,19,22; 88:1  <b>smaller</b> 67:10; 84:11  <b>smallest</b> 41:11  <b>Social</b> 53:9; 57:13; 74:16; 85:3  <b>society</b> 58:22; 67:18; 87:23  <b>software</b> 12:18; 82:15; 86:3  <b>solely</b> 30:1,13  <b>solid</b> 67:16  <b>solution</b> 66:21  <b>solutions</b> 15:10; 48:6; 75:12; 86:20  <b>solve</b> 66:13  <b>Somebody</b> 64:4  <b>somehow</b> 36:17; 57:17  <b>someone</b> 52:8; 56:9; 58:18; 65:4; 68:7; 72:3; 88:8  <b>something</b> 25:20; 30:15; 45:22; 54:24  <b>Sometimes</b> 69:7  <b>somewhat</b> 67:12; 68:6; 72:18  <b>soon</b> 37:19  <b>sorry</b> 20:15; 88:7,10,12  <b>sort</b> 17:3; 67:16,22  <b>sorts</b> 24:20  <b>sought</b> 34:8  <b>speak</b> 69:21  <b>speaker</b> 24:10  <b>Speaker's</b> 6:16; 9:16,24; 10:2; 91:3</p>
---	--	--	---

Speakers 10:9; 45:15; 47:15  
 specific 22:16; 34:7; 40:5; 46:8; 47:13; 51:14; 67:12; 71:21; 75:10  
 specifically 58:3; 74:11,12  
 specifics 67:15  
 speed 25:12; 68:3  
 spell 10:3  
 spend 41:7; 49:24; 89:2  
 spent 32:22; 89:4  
 spoken 64:20  
 ss 92:3  
 stable 67:7  
 Staff 70:20; 82:17; 84:12; 86:6,8; 88:6,18,19; 89:14; 90:7,19  
 Stakeholder 4:4; 45:15; 47:20; 50:12  
 stakeholders 14:16  
 stand 51:1  
 standard 12:24; 13:12; 78:23  
 Standards 1:9; 3:17; 32:6,8; 34:12; 35:1,10; 36:7; 39:19; 40:24; 41:3,6; 43:10; 46:10,11; 63:5; 87:4,9  
 Standards' 36:2  
 standpoint 25:9  
 stands 44:8; 89:24  
 stark 14:12  
 start 28:18; 64:24  
 started 6:4; 10:9; 22:8; 85:14  
 State 5:13; 14:6,10,18; 20:8,23; 24:19,24; 28:3,24; 29:13; 34:11,13; 44:3; 47:16,19; 61:20,21,24; 62:12,21; 63:5,11; 65:19; 69:8  
 State's 6:12; 14:19; 44:1  
 state- 12:16  
 stated 47:7; 54:13  
 Statement 4:2,4,16,19,24,26; 5:7,23,24; 30:12; 72:17  
 Statements 30:18  
 States 13:14; 25:10,24; 26:10; 31:9; 39:9,12; 47:14; 60:1  
 States' 34:14  
 Statewide 45:1  
 Statute 17:6; 49:14; 72:2  
 Statutory 38:16  
 stay 55:2; 72:20  
 Stenographer 10:3  
 step 11:17; 18:12; 29:10; 74:6  
 step-by-step 22:9,20  
 steps 19:12; 26:1,2,3; 82:2; 85:6  
 Steven 4:8,10  
 sticking 71:13  
 stop 58:20  
 storage 76:3  
 store 54:20; 58:19; 60:18  
 stored 38:22  
 stores 25:12  
 storm 50:3  
 straightforward 12:20  
 strategies 90:18

Strategist 4:11  
 streamlining 11:24  
 streams 82:24  
 stress 32:10  
 striving 84:24  
 strongly 14:22; 43:17  
 struggling 55:2; 57:21  
 student 83:2; 85:3; 88:17  
 student's 85:3  
 students 81:17; 82:3; 85:1,17; 86:24; 88:3  
 study 46:18; 83:12; 86:11,16  
 stuff 66:14  
 Sub 8:24  
 subject 6:22; 30:9; 36:24; 37:2,10; 39:5,9; 40:8; 43:21; 74:23  
 Submissions 1:3  
 submit 39:13; 42:23; 73:11  
 submitted 51:23  
 Subsection 12:12  
 subsequent 17:12  
 substance 33:6; 43:6; 62:3  
 substantial 66:7; 76:1; 82:12  
 substantially 42:8  
 substantive 71:21  
 sufficient 38:20  
 suggest 18:16; 26:22; 38:11; 47:21; 53:14; 85:19  
 suggested 43:8  
 suggestion 69:5  
 suggestions 11:23; 22:18; 48:16  
 suggests 12:2  
 Suite 2:4  
 SUPERVISION 92:24  
 support 42:15; 48:3; 49:8,18; 70:23; 81:22; 87:6; 88:20  
 supported 13:13  
 supporting 86:7  
 supposed 17:20  
 survive 32:17; 90:18  
 suspect 21:20  
 suspend 20:11; 59:17  
 sustainable 86:20  
 Sweeney 3:7; 4:27; 73:4,6,8,9  
 sweeping 85:24  
 sync 25:18; 26:3  
 synced 26:18  
 system 90:12  
 systems 12:17; 13:1; 27:9,17,18; 32:23; 36:17; 49:20; 75:7; 76:3; 88:5,15; 89:20,22; 90:13

**T**

table 6:16,16; 9:16,24,24; 58:17  
 taken 1:11; 14:13; 32:10; 59:5; 85:6; 92:8,9  
 takers 21:24  
 takes 43:6; 55:19  
 taking 26:2,3; 65:19; 82:1  
 Tami 2:16; 4:14; 30:22,23; 31:1,3

tapes 19:6  
 task 89:11  
 tasked 26:14  
 tax 57:14; 67:21  
 team 73:16  
 tech 10:22,23  
 technical 27:5  
 technically 12:11  
 technologies 12:23; 13:2; 33:2; 46:8; 75:11,16,19  
 Technology 4:3; 5:6; 10:21; 12:6,16; 13:14; 14:8,18,24; 65:19; 66:12; 67:6; 75:10; 82:15; 88:24; 90:11  
 tell 69:16  
 ten 54:3; 56:15; 61:24; 63:20  
 tenant 68:9  
 tend 65:10  
 tens 32:22  
 term 14:17; 76:15  
 terms 14:17; 40:17; 75:15  
 testified 33:24; 60:20  
 testify 10:1,6; 16:12; 51:13; 73:17; 80:24  
 testifying 10:3; 53:4  
 testimonies 38:3  
 Testimony 4:9,12,14; 5:5,13; 6:23; 8:14; 9:7; 17:23; 41:9; 51:24; 73:12  
 thank 11:1,5; 15:20,21,23; 23:4,5,7; 30:21,23; 44:7,11; 50:19; 52:11,14,15,19; 59:20; 61:4,5,7,9; 64:1,2,6,8; 69:22,23; 70:1; 73:3,14,14,19,20; 80:22,23; 81:3,20; 87:11,12,17; 88:9; 90:24; 91:2,7  
 Thanks 15:14,17; 30:20; 50:22; 88:12  
 that's 6:10; 15:18; 56:4; 66:8; 67:16; 69:3; 91:3  
 theft 11:12; 14:12; 22:9; 48:23; 58:21; 60:10  
 themselves 10:4; 39:5; 69:12  
 there'll 68:16  
 there's 18:7; 24:12; 63:10; 66:20; 69:8; 90:1  
 They'll 82:16  
 they're 12:23; 17:19; 57:3; 76:8; 77:1; 85:11,11; 89:21; 90:21  
 they've 14:13; 85:14  
 thing 28:19; 29:6,9  
 things 57:4; 64:23; 65:6,15,17; 66:4; 68:5,14; 71:2  
 think 6:5; 11:9; 13:20; 15:9; 18:2; 22:1,18; 24:10,12; 26:10; 29:1,1,6,8; 64:22; 66:3,10; 67:3,6,8; 68:23; 69:1; 71:2,15; 74:6; 75:18; 86:9  
 third 7:5; 8:20; 13:17; 19:14; 29:2,3; 39:7; 57:22; 84:17  
 third- 27:21; 83:14  
 third-parties 53:21  
 Third-Party 13:17; 28:2,15; 37:3; 40:6; 49:6; 57:24; 76:9; 77:6; 83:16;

84:7  
 thought 72:15; 86:14  
 thoughtful 75:20  
 thousand 17:18; 76:19; 88:3  
 thousands 56:22; 57:18; 83:21  
 threats 33:1  
 three 22:12; 48:9; 55:12; 65:23; 66:18; 70:17; 88:6,18  
 throughout 65:22; 81:15  
 throw 28:17; 69:4  
 Thumb 19:5  
 tied 71:20  
 Tim 73:4,9  
 time 14:3; 15:3,6; 24:5; 25:2,5; 27:17,17; 29:15,19; 33:11; 36:12; 37:12,22; 38:3,9; 42:21; 44:5,7; 45:11; 50:1,7,14; 51:19; 55:11,20; 57:2,7; 59:12; 60:21; 66:24; 68:12,15; 76:22; 79:2; 80:8,23; 82:20; 83:12; 84:6,6,16; 85:8,15; 86:21; 87:3,4; 89:2,4,6,19  
 time- 49:16  
 time-consuming 86:4  
 timeline 82:9  
 times 17:22; 50:3; 75:23  
 timing 48:12  
 Timothy 3:7; 4:27; 73:6,8  
 today 11:19; 31:4; 32:2,6; 33:4,10; 35:4; 38:4; 47:23; 51:11,17,22; 52:1,2; 53:15; 54:16; 55:11; 62:7; 71:16; 75:23; 91:1  
 today's 35:7,7  
 together 43:2; 66:18  
 told 27:16; 74:13  
 took 24:22; 25:1; 42:19  
 total 31:10,20,23  
 touched 67:11  
 tough 50:3  
 toward 80:18; 90:5  
 towards 83:1  
 Towns 28:23; 29:14  
 trade 10:22; 36:13; 45:1; 61:18; 70:14  
 tradition 10:6  
 train 90:7  
 training 13:23  
 transaction 43:12; 78:19  
 transactions 78:15  
 transcribed 92:10  
 transcript 92:12,22  
 transfer 69:7  
 transference 69:12  
 transmissions 12:21  
 transmitted 12:8,10  
 transport 55:18  
 Transportation 1:15; 8:9  
 travel 12:9  
 traveling 67:19  
 Treasurers 34:12  
 treated 74:15,17  
 trees 60:4,6  
 true 50:4; 56:19; 92:12  
 truly 14:20; 46:17; 52:5  
 trust 32:16,17  
 try 25:15; 83:10  
 trying 16:24; 25:11;

27:2,3; 29:12; 49:24; 50:2; 53:13; 56:24; 83:6; 85:10,11,20  
**TWO** 9:19; 22:12; 23:17; 24:22; 30:17; 36:2,17,20; 40:21; 42:19; 48:9,17; 50:15; 62:9; 66:18; 72:6; 87:9  
**type** 25:22; 26:22; 27:21; 38:21; 47:23; 57:5; 59:4; 80:5  
**types** 12:20; 55:2

**U**

**U.K.** 22:14  
**U.S** 31:7; 39:8  
**ultimately** 21:8  
**unanimous** 43:15  
**unaware** 66:8  
**uncertainties** 80:13  
**uncertainty** 74:21  
**unclear** 13:11  
**undefined** 40:17  
**underlying** 86:18  
**undermine** 67:23  
**undermines** 37:20  
**Undersecretary** 4:7; 5:11; 11:1; 47:22; 73:15; 81:24; 87:2  
**understand** 18:17; 19:4; 37:6; 40:21; 71:14; 90:7,11  
**understanding** 72:11; 75:14; 78:10  
**understood** 25:3  
**undertake** 41:5; 49:20  
**undertaking** 84:8; 85:5  
**undertook** 33:7  
**unduly** 42:3; 83:17  
**unfunded** 82:12,19  
**Union** 3:6; 4:24; 70:9,13,18  
**Unions** 70:14; 71:9; 72:4,5,10  
**universally** 12:24  
**Universities** 5:2; 81:13,15,22; 82:7,13,21; 83:9,20; 84:19,23  
**unless** 12:11; 72:23; 92:23  
**Unlike** 42:5; 74:18  
**unnecessarily** 60:9  
**unnecessary** 49:7  
**unprecedented** 14:2  
**unresolved** 40:15  
**unsuccessful** 35:3  
**unwilling** 77:3  
**unwillingness** 40:4  
**unworkable** 16:16; 41:24; 76:23; 79:17  
**up-** 76:1  
**update** 50:15  
**updated** 18:13  
**upgrade** 27:9,13,17; 75:3  
**upon** 37:16; 44:5; 45:7; 46:3,11,20  
**upset** 68:6  
**upwards** 21:7  
**urge** 45:13; 48:14; 50:9; 51:13,21; 52:11; 60:13,13  
**use** 7:5; 55:11  
**used** 13:4; 43:10; 49:9;

60:24; 74:15,19; 75:16  
**useful** 18:11; 21:15; 22:5,17  
**users** 90:11  
**uses** 85:2  
**using** 43:18  
**usually** 57:15  
**Utilities** 74:15  
**utilizes** 78:18

**V**

**V.P** 2:21  
**vague** 34:24; 67:17,22  
**value** 65:6,14; 82:23  
**variety** 23:19  
**various** 34:9; 48:6  
**vast** 54:13  
**Vendor** 3:4; 19:14; 40:6; 64:11,17; 76:9,10,19; 77:1,1,6,13; 78:17,18; 89:8,22; 90:1,16  
**Vendors** 19:18,23; 76:10,24; 77:24; 78:8; 83:22; 84:8; 90:19,20  
**vendors'** 90:3  
**verification** 83:15  
**Vernon** 5:13  
**version** 25:17; 42:9  
**viability** 76:16  
**Vice** 4:17,20; 5:7,22; 44:21; 81:11  
**victims** 62:2  
**viewed** 80:11  
**vigorous** 47:20  
**violence** 62:2  
**virtually** 82:6; 84:10; 85:2  
**volume** 84:19; 85:16  
**voluntary** 20:22  
**vulnerabilities** 33:1  
**vulnerable** 63:21

**W**

**wager** 17:17  
**want** 10:24; 11:20; 23:17; 24:6,6; 30:2; 32:9; 35:10; 40:20; 41:18; 48:8; 56:5; 81:20  
**wants** 91:4  
**wasn't** 26:12; 29:11  
**waste** 38:3  
**ways** 12:2; 20:3,3  
**we'd** 13:15; 25:5; 29:17,23; 58:20; 73:20; 89:24  
**we're** 15:11; 20:1; 24:4,5; 28:14,14,22; 30:6; 56:24; 59:19; 62:9,9; 90:12,21  
**We've** 13:13; 23:24; 41:20; 89:12  
**weather** 50:3  
**website** 18:16,22  
**Wednesday** 9:9  
**weeks** 15:13  
**weigh** 11:20  
**WEINSTEIN** 2:24; 52:23; 53:3  
**well-crafted** 11:14  
**well-reasoned** 42:17  
**went** 42:7  
**Weymouth** 1:21

**what'll** 69:13  
**whatever** 17:11; 18:5,20; 63:6  
**wheel** 43:9  
**whereby** 49:19  
**WHEREOF** 92:17  
**whether** 25:21; 26:20; 56:24; 57:4; 68:20  
**who'd** 21:21  
**whole** 27:24; 60:24; 68:18; 90:4  
**wholeheartedly** 43:13; 48:3  
**wholly** 39:3  
**whom** 18:9; 35:13; 67:2  
**whose** 59:10  
**why** 16:15,17; 19:19; 29:14; 32:23; 37:6; 70:2; 72:19  
**wide** 23:19; 24:14; 84:14  
**wide-reaching** 14:6  
**widely** 13:3; 84:21  
**widespread** 80:8  
**will** 6:5; 7:20; 8:6; 9:4,8; 10:6; 12:9; 16:14; 18:6,12,13,22; 21:11; 30:17; 36:1; 38:3,5; 39:1,2; 41:12; 45:7; 46:13,24; 49:16,23; 54:22,24; 59:5,11; 60:21; 66:21; 68:6; 69:4,13; 73:13; 80:7; 82:13; 84:5,9,15; 86:2,7,21; 87:3  
**willing** 15:7; 21:21; 39:4,13; 50:16; 52:7  
**willingness** 73:17  
**wireless** 12:21  
**wirelessly** 12:11  
**wish** 10:6  
**wishing** 10:1  
**withdraw** 74:19  
**withdrawal** 43:19  
**within** 26:15; 49:13; 57:6,18; 63:11; 74:7; 84:20; 88:23; 92:11  
**without** 13:10; 14:7; 40:7; 43:1; 47:9; 59:7; 74:3  
**WITNESS** 92:17  
**won't** 15:6  
**Worcester** 60:4  
**work** 14:24; 15:12; 17:11,11,14; 18:8; 23:23; 24:24; 30:18; 44:8; 50:16; 56:1; 64:15; 66:6; 70:19; 73:1; 90:5  
**workable** 12:1; 14:20; 15:10; 77:11  
**worked** 21:7; 72:1  
**working** 43:2; 50:21; 52:16; 57:3; 80:18; 85:10  
**works** 16:22; 72:7  
**World** 13:5,24; 16:10; 28:4; 65:9,22  
**worthwhile** 18:6; 26:11  
**wouldn't** 90:13  
**wringing** 25:11  
**write** 17:7; 28:1; 66:19  
**writing** 39:6  
**Written** 1:3; 8:14; 9:7,7,11; 15:4,5,15; 23:18; 46:6; 48:20; 49:5; 55:23; 56:5; 58:24; 60:3; 89:9  
**wrongful** 53:20; 58:21  
**wrote** 34:15

**Y**

**yeah** 69:3  
**year** 6:14; 7:3,3; 19:16,23; 37:19; 48:18; 50:15; 55:6; 60:19; 71:19; 86:11,17; 87:9  
**years** 20:24; 21:8,12,16; 24:22; 27:12; 36:2; 42:19; 63:7; 75:24; 84:1  
**yet** 79:16  
**you'd** 21:24  
**you'll** 13:18; 15:10  
**you're** 18:20; 19:7,15; 27:11; 87:15  
**you've** 53:15; 58:2; 68:21; 70:24; 71:4; 82:4  
**yourself** 25:15; 47:23; 70:20

[

[Confusion/Noise] 20:10  
[Door] 64:5  
[EXHIBIT] 6:17; 9:19  
[Inaudible] 81:2  
[Laughter/Comments] 22:3  
[Laughter] 21:23; 64:13  
[No] 10:8; 91:6  
[Off] 20:14; 44:13