DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

COMMONWEALTH OF MASSACHUSETTS
OFFICE OF CONSUMER AFFAIRS & BUSINESS REGULATION
10 Park Plaza, Suite 5170 Boston, MA 02116
(617) 973-8700 FAX (617) 973-8799
www.mass.gov/consumer

GREGORY BIALECKI
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

BARBARA ANTHONY
UNDERSECRETARY OF CONSUMER AFFAIRS AND BUSINESS REGULATION

For immediate release, Aug. 17, 2009

CONTACT:
Jason Lefferts
(617) 973-8767

Small-Business Considerations Reflected in Massachusetts' Revised ID Theft Regulations

Changes balance consumer protections with business concerns

BOSTON – Aug. 17, 2009 – In keeping with Governor Deval Patrick's commitment to balancing consumer protection with the needs of small business owners, Massachusetts Undersecretary of the Office of Consumer Affairs and Business Regulation Barbara Anthony today announced adjustments to Massachusetts' identity theft regulations that maintain protections and also reinforce flexibility in compliance by small businesses.

The updated regulations will take effect March 1, 2010. The regulations make clear that their approach to data security is a risk-based approach that is especially important to small businesses that may not handle a lot of personal information about customers. Under a risk-based approach, a business, in developing a written security program, should take into account its size, nature of its business, the kinds of records it maintains, and the risk of identity theft posed by its operations.

"In listening to the concerns of small business leaders, we understand there were issues regarding the impact these regulations have on those companies," said Undersecretary Anthony. "These updated regulations feature a fair balance between consumer protections and business realities."

New language in the regulations recognizes that the size of a business and the amount of personal information it handles plays a role in the data security plan the business creates. The new language requires safeguards that are appropriate to the size, scope and type of business handling the information; the amount of resources available to the business; the amount of stored data; and the need for security and confidentiality of both consumer and employee information.

The changes, Anthony said, make clear the regulations are risk-based in implementation, not just in enforcement as had been the case in earlier versions of the regulations. In addition, the

regulations are technology neutral and acknowledge that technical feasibility plays a role in what many businesses, especially small businesses can do to protect data. The overall approach is more consistent with federal law, she said.

“Whether it’s a small amount of employee paperwork, or a large amount of consumer information kept on an electronic database, each requires its own appropriate level of security and protection,” Anthony said. “The changes we are making reflect that reality without exposing companies or consumers to a heightened risk of theft.”

The regulations are a product of the identity theft prevention law signed by Governor Deval Patrick. Governor Patrick signed an executive order last September requiring all state agencies to implement security measures consistent with the requirements in the regulations.

The Office of Consumer Affairs and Business Regulation today sent to the Secretary of State notice of public hearing on the changes. That hearing will be held on Tuesday, Sept. 22, at 10 a.m. at the Transportation Building, 10 Park Plaza, Boston.

For more information about identity theft protection, visit the Office of Consumer Affairs and Business Regulation website, www.mass.gov/consumer.

###

DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

COMMONWEALTH OF MASSACHUSETTS
OFFICE OF CONSUMER AFFAIRS & BUSINESS REGULATION
10 Park Plaza, Suite 5170 Boston, MA 02116
(617) 973-8700 FAX (617) 973-8799
www.mass.gov/consumer

GREGORY BIALECKI
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

BARBARA ANTHONY
UNDERSECRETARY OF CONSUMER AFFAIRS AND BUSINESS REGULATION

Frequently Asked Question Regarding 201 CMR 17.00

What are the differences between this version of 201 CMR 17.00 and the version issued in February of 2009?

There are some important differences in the two versions. First, the most recent regulation issued in August of 2009 makes clear that the rule adopts a risk-based approach to information security, consistent with both the enabling legislation and applicable federal law, especially the FTC's Safeguards Rule. A risk-based approach is one that directs a business to establish a written security program that takes into account the particular business' size, scope of business, amount of resources, nature and quantity of data collected or stored, and the need for security. It differs from an approach that mandates every component of a program and requires its adoption regardless of size and the nature of the business and the amount of information that requires security. This clarification of the risk based approach is especially important to those small businesses that do not handle or store large amounts of personal information. Second, a number of specific provisions required to be included in a business's written information security program have been removed from the regulation and will be used as a form of guidance only. Third, the encryption requirement has been tailored to be technology neutral and technical feasibility has been applied to all computer security requirements. Fourth, the third party vendor requirements have been changed to be consistent with Federal law.

To whom does this regulation apply?

The regulation applies to those engaged in commerce. More specifically, the regulation applies to those who collect and retain personal information in connection with the provision of goods and services or for the purposes of employment. The regulation does not apply, however, to natural persons who are not in commerce.

Does 201 CMR 17.00 apply to municipalities?

No. 201 CMR 17.01 specifically excludes from the definition of "person" any "agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof." Consequently, the regulation does not apply to municipalities.

Must my information security program be in writing?

Yes, your information security program must be in writing. The scope and complexity of the document will vary depending on your resources, and the type of personal information you are

storing or maintaining. But, everyone who owns or licenses personal information must have a written plan detailing the measures adopted to safeguard such information.

What about the computer security requirements of 201 CMR 17.00?

All of the computer security provisions apply to a business if they are technically feasible. The standard of technical feasibility takes reasonableness into account. (See definition of "technically feasible" below.) The computer security provisions in 17.04 should be construed in accordance with the risk-based approach of the regulation.

Does the regulation require encryption of portable devices?

Yes. The regulation requires encryption of portable devices where it is reasonable and technically feasible. The definition of encryption has been amended to make it technology neutral so that as encryption technology evolves and new standards are developed, this regulation will not impede the adoption of such new technologies.

Do all portable devices have to be encrypted?

No. Only those portable devices that contain personal information of customers or employees and only where technically feasible The "technical feasibility" language of the regulation is intended to recognize that at this period in the development of encryption technology, there is little, if any, generally accepted encryption technology for most portable devices, such as cell phones, blackberries, net books, iphones and similar devices. While it may not be possible to encrypt such portable devices, personal information should not be placed at risk in the use of such devices. There is, however, technology available to encrypt laptops.

Must I encrypt my backup tapes?

You must encrypt backup tapes on a prospective basis. However, if you are going to transport a backup tape from current storage, and it is technically feasible to encrypt (i.e. the tape allows it) then you must do so prior to the transfer. If it is not technically feasible, then you should consider the sensitivity of the information, the amount of personal information and the distance to be traveled and take appropriate steps to secure and safeguard the personal information. For example, if you are transporting a large volume of sensitive personal information, you may want to consider using an armored vehicle with an appropriate number of guards.

What does "technically feasible" mean?

"Technically feasible" means that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used.

Must I encrypt my email if it contains personal information?
If it is not technically feasible to do so, then no. However, you should implement best practices by not sending unencrypted personal information in an email. There are alternative methods to communicate personal information other through email, such as establishing a secure website that requires safeguards such as a username and password to conduct transactions involving personal information.

Are there any steps that I am required to take in selecting a third party to store and maintain personal information that I own or license?
You are responsible for the selection and retention of a third-party service provider who is capable of properly safeguarding personal information. The third party service provider provision in 201 CMR 17.00 is modeled after the third party vendor provision in the FTC's Safeguards Rule.

I have a small business with ten employees. Besides my employee data, I do not store any other personal information. What are my obligations?
The regulation adopts a risk-based approach to information security. A risk-based approach is one that is designed to be flexible while directing businesses to establish a written security program that takes into account the particular business's size, scope of business, amount of resources and the need for security. For example, if you only have employee data with a small number of employees, you should lock your files in a storage cabinet and lock the door to that room. You should permit access to only those who require it for official duties. Conversely, if you have both employee and customer data containing personal information, then your security approach would be more stringent. If you have a large volume of customer data containing personal information, then your approach would be even *more* stringent.

Except for swiping credit cards, I do not retain or store any of the personal information of my customers. What is my obligation with respect to 201 CMR 17.00?
If you use swipe technology only, and you do not have actual custody or control over the personal information, then you would not own or license personal information with respect to *that* data, as long as you batch out such data in accordance with the Payment Card Industry (PCI) standards. However, if you have employees, see the previous question.

Does 201 CMR 17.00 set a maximum period of time in which I can hold onto/retain documents containing personal information?
No. That is a business decision you must make. However, as a good business practice, you should limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected and limit the time such information

is retained to that reasonably necessary to accomplish such purpose. You should also limit access to those persons who are reasonably required to know such information.

Do I have to do an inventory of all my paper and electronic records?
No, you do not have to inventory your records. However, you should perform a risk assessment and identify which of your records contain personal information so that you can handle and protect that information.

How much employee training do I need to do?
There is no basic standard here. You will need to do enough training to ensure that the employees who will have access to personal information know what their obligations are regarding the protection of that information, as set forth in the regulation.

What is a financial account?
A financial account is an account that if access is gained by an unauthorized person to such account, an increase of financial burden, or a misappropriation of monies, credit or other assets could result. Examples of a financial account are: checking account, savings account, mutual fund account, annuity account, any kind of investment account, credit account or debit account.

Does an insurance policy number qualify as a financial account number?
An insurance policy number qualifies as a financial account number if it grants access to a person's finances, or results in an increase of financial burden, or a misappropriation of monies, credit or other assets.

I am an attorney. Do communications with clients already covered by the attorney-client privilege immunize me from complying with 201 CMR 17.00?
If you own or license personal information, you must comply with 201 CMR 17.00 regardless of privileged or confidential communications. You must take steps outlined in 201 CMR 17.00 to protect the personal information taking into account your size, scope, resources, and need for security.

I already comply with HIPAA. Must I comply with 201 CMR 17.00 as well?
Yes. If you own or license personal information about a resident of the Commonwealth, you must comply with 201 CMR 17.00, even if you already comply with HIPAA.

What is the extent of my "monitoring" obligation?
The level of monitoring necessary to ensure your information security program is providing protection from unauthorized access to, or use of, personal information, and effectively limiting risks will depend largely on the nature of your business, your business practices, and the

amount of personal information you own or license. It will also depend on the form in which the information is kept and stored. Obviously, information stored as a paper record will demand different monitoring techniques from those applicable to electronically stored records. In the end, the monitoring that you put in place must be such that it is reasonably likely to reveal unauthorized access or use.

Is everyone's level of compliance going to be judged by the same standard?
Both the statute and the regulations specify that security programs should take into account the size and scope of your business, the resources that you have available to you, the amount of data you store, and the need for confidentiality. This will be judged on a case by case basis.

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

Section:

17.01 **Purpose and Scope**

(1) Purpose
This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are 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.

(2) Scope
The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

17.02: **Definitions**

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

Breach of security, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

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

Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owns or licenses, receives, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person, a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

Personal information, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record or Records, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider, any person that receives, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation; provided, however, that "Service provider" shall not include the U.S. Postal Service.

17.03: **Duty to Protect and Standards for Protecting Personal Information**

(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (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. 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 or licenses such information may be regulated.
(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:
(a) Designating one or more employees to maintain the comprehensive information security program;
(b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:
1. ongoing employee (including temporary and contract employee) training;
2. employee compliance with policies and procedures; and
3. means for detecting and preventing security system failures.
(c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.
(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.
(e) Preventing terminated employees from accessing records containing personal information.
(f) Oversee service providers, by:
1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and
2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that any contract a person has entered into with a third party service provider prior to March 1, 2012, shall be deemed to be in compliance herewith, notwithstanding the absence in any such contract of a requirement that the service provider maintain such protective security measures, so long as the contract was entered into before March 1, 2010.
(g) Reasonable restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.
(h) 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.
(i) 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.
(j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

17.04: **Computer System Security Requirements**

Every person that owns or licenses 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, and to the extent technically feasible, 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)Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
(5) Encryption of all personal information stored on laptops or other portable devices;
(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**

(1)Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

REGULATORY AUTHORITY

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

COMMONWEALTH OF MASSACHUSETTS
OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION
TEN PARK PLAZA
BOSTON, MA 02116
(617) 973-8700
www.mass.gov/oca

DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

GREGORY BIALECKI
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

BARBARA ANTHONY
UNDERSECRETARY
OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION

NOTICE OF PUBLIC HEARING

Pursuant to the provisions of M.G.L. c. 30A, and the authority granted to the Undersecretary of the Office of Consumer Affairs and Business Regulation under M.G.L. c. 93H, the Office of Consumer Affairs and Business Regulation will hold a public hearing in connection with the promulgation of 201 CMR 17.00, concerning the protection of personal information of residents of the Commonwealth. The public hearing will commence at 10:00 a.m. on Tuesday September 22, 2009, in Room No. 5-6, Second Floor of the Transportation Building, Ten 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 201 CMR 17.00, *Standards for the Protection of Personal Information of Residents of the Commonwealth*. The purpose of 201 CMR 17.00 is to implement the provisions of M.G.L c. 93H relative to the standards to be met by those who own or license personal information about a resident of the Commonwealth. The regulation establishes standards for safeguarding such information, in paper and electronic records, in order to protect its security and confidentiality in a manner consistent with industry standards, to protect against threats and hazards to the security of such information, and to protect against unauthorized access to or use of such information in a manner that may result in substantial harm or inconvenience to any consumer.

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 September 25, 2009. Such written comments may be mailed to: Office of Consumer Affairs and Business Regulation, 10 Park Plaza, Suite 5170, Boston, MA 02116, Attention: Jason Egan, Deputy General Counsel, or e-mailed to Jason.Egan@state.ma.us.

Copies of the proposed regulation may be obtained from the Office of Consumer Affairs and Business Regulation website, or by calling (617) 973-8700.

August 17, 2009

/s/ Barbara Anthony, Undersecretary
Office of Consumer Affairs and Business Regulation