

## MASSACHUSETTS ADOPTS COMPREHENSIVE PRIVACY REGULATIONS

By: *Laurel Van Buskirk*  
Email: [lvanbuskirk@devinemillimet.com](mailto:lvanbuskirk@devinemillimet.com)  
Phone: 603.695.8565

JUNE 5, 2009

In the past several years, high profile security breaches of sensitive consumer data at large companies like TJX Companies, Hannaford Brothers, and Heartland Payment Systems, among others, have increased awareness of the relative insecurity of personal information in the age of technology. As a result, several states, including Massachusetts, have enacted or strengthened laws regarding the handling of consumer data. These laws also delineate the merchants' legal liability in the event of a breach. While these laws are generally aimed at protecting consumers, their expansive provisions often apply to all personal data, including personal information held by employers. As addressed more fully below, the promulgation of new regulations in Massachusetts may have a large impact on Massachusetts employers.

Employers are required to maintain all types of records on job applicants, employees, and former employees. These records contain a wealth of personal information gleaned from a variety of sources. Some of this information may be obtained through the use of a consumer reporting agency, while some of it is obtained directly from the individual on his/her application for employment, benefits paperwork, the I-9 Form, a W-2, payroll records and other paperwork incidental to employment. It is exactly this type of paperwork maintained by employers that will be subject to the laws aimed at protecting consumer information.

While most states already have laws in place requiring notification to consumers following a security breach, Massachusetts is one of several states that has also strengthened provisions requiring companies to take proactive measures to secure personal information. 201 Massachusetts Code of Regulations ("MCR") 17, *et seq.* : *Standards for the Protection of Personal Information of Residents of the Commonwealth*, implements the provisions of Massachusetts General Law, Chapter 93H, relative to the standards

### Labor, Employment & Employee Benefits

**Mark Broth, Chair**  
603.695.8558  
[mbroth@devinemillimet.com](mailto:mbroth@devinemillimet.com)

**Aaron Gilman**  
978.475.9100  
[agilman@devinemillimet.com](mailto:agilman@devinemillimet.com)

**Newton Kershaw**  
603.695.8571  
[nkershaw@devinemillimet.com](mailto:nkershaw@devinemillimet.com)

**Karen Levchuk**  
603.695.8618  
[klevchuk@devinemillimet.com](mailto:klevchuk@devinemillimet.com)

**Patricia McGrath**  
603.695.8537  
[pmcgrath@devinemillimet.com](mailto:pmcgrath@devinemillimet.com)

**Anthony Augeri**  
978.475.9100  
[aaugeri@devinemillimet.com](mailto:aaugeri@devinemillimet.com)

**Margaret O'Brien**  
603.695.8631  
[mobrien@devinemillimet.com](mailto:mobrien@devinemillimet.com)

**Anne Scheer**  
603.410.1708  
[ascheer@devinemillimet.com](mailto:ascheer@devinemillimet.com)

**Laurel Van Buskirk**  
603.695.8565  
[lvanbuskirk@devinemillimet.com](mailto:lvanbuskirk@devinemillimet.com)

**Anne Trevethick**  
603.695.8725  
[atrevethick@devinemillimet.com](mailto:atrevethick@devinemillimet.com)

DEVINEMILLIMET.COM

EMPLOYMENT@DEVINEMILLIMET.COM

to be met by persons who own, license, store or maintain personal information about a resident of the Commonwealth. 201 MCR 17.03-1705. Specifically, 17.03 requires that:

[e]very person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information.

“Personal information” includes a Massachusetts resident’s first and last name or first initial and last name in combination with his/her social security number, driver’s license number, state-issued identification card number, financial account number, or credit or debit card number. The only exceptions are if the information was lawfully obtained from publicly available information or from federal, state or local government records made available to the general public. 201 CMR 17.02. Consequently, any employer that employs a Massachusetts resident conceivably could be held responsible for compliance with this ruling (although it is unclear how Massachusetts would enforce its rules against an employer located outside of the state).

Essentially, the regulations establish minimum standards to be met in order to safeguard personal information contained in both paper and electronic records. All affected companies must be in full compliance with the regulation on or before January 1, 2010. The regulation is enforced by the Massachusetts Attorney General.

Development of Security Programs. Employers will be required to develop a comprehensive, written information security program (CISP) that is consistent with industry standards and that contains administrative, technical and physical safeguards to ensure the security and confidentiality of those records. The CISP must also be consistent with safeguards for protection of personal information set forth in any state or federal regulations by which the employer is regulated.

As the rule recognizes that CISPs may vary, depending on the size, scope and type of business of the “person” obligated to safeguard the personal information; the resources available to the person; and the amount of data stored, employers and companies complying with these rules have some leeway. Obviously, a ten person company may not be held to the same technological standards as a five hundred person company. However, since the thrust of this ruling is a recognition of the need for security and confidentiality of both consumer and employee information, employers of all

#### Office Locations:

111 Amherst Street  
Manchester, NH 03101  
T 603.669.1000  
F 603.669.8547

300 Brickstone Square  
Andover, MA 01810  
T 978.475.9100  
F 978.470.0618

43 North Main Street  
Concord, NH 03301  
T 603.226.1000  
F 603.226.1001



sizes would be required to put thought and effort into compliance. Regardless of size, however, the rule contemplates that an effective CISP will develop and implement written policies addressing all the items below. See 201 MCR 17.03.

*Identify a point person.* Under the rules, businesses must identify a person or a team of people to be responsible for the CISP. This means that in order to comply with this rule, every business must designate a specific individual or team who are responsible for design, implementation, coordination and maintenance of the plan.

*Identify Risks.* The first step in developing a security program is identifying the personal information that a business stores, including understanding which records and documents likely contain personal information and where those records are stored. Employers should assess the risks to those records and how they're stored. Is the information secure? Is it kept confidential? Employers should evaluate how effective current safeguards are at protecting the information, including training procedures, employee compliance with current procedures and policies, and whether information systems need to be upgraded. Employers should evaluate not only the safety and security of electronic records, but physical records as well. For example, are filing cabinets containing Form I-9s or employee paperwork kept locked? Is your internet system secure?

*Know Your Information.* In addition to knowing what personal information is stored and where it is stored, businesses should understand why they have the information and develop policies to manage that personal information. These include policies to ensure that employees only collect the minimum amount of personal information necessary to accomplish the business need, retention policies to ensure that the information is maintained for the minimum amount of time (but no longer); and limiting access to the stored information to as few employees as possible.

*Specific Policies for Specific Circumstances.* Design security policies that address the realities of employees working from home. This includes policies relative to what types of documents employees are allowed to bring home and what they're allowed to access from home.

*Know the Policies.* Businesses must train their employees on any security policies they implement, including how to handle and dispose of personal information. This includes a variety of policies including collecting the minimum amount of information, to computer security, to their obligation of confidentiality. Employees must understand their obligations to protect the personal information of customers and other employees. Businesses should regularly monitor and audit employees who access personal



information to ensure both that employees are complying with company security policies and that safeguards are effectively working.

*Third Parties.* Businesses must take reasonable steps to verify that third-party service providers with access to personal information are able to adequately protect that information. This means that businesses should choose vendors that are capable of maintaining safeguards for personal information, contractually require vendors to maintain such safeguards, and should do their homework and require written confirmation that the vendor also has a comprehensive CISP.

*Former Employees.* Limit access of terminated employees to personal information. This means developing policies concerning post-termination procedures, including, if appropriate, an escort to pick-up personal belongings and out of the building. Additionally, electronic access passwords or swipe cards should be deactivated.

*Stay Vigilant.* Businesses must regularly monitor and audit their systems to ensure that all electronic and physical security measures are in tact and functioning properly.

*Enforcement.* Rules and policies are only effective if they are followed. Companies must implement measures to monitor policy compliance and set disciplinary consequences for employee non-compliance. Businesses should document any responses to non-compliance.

*Document.* Document responsive actions to any security breach or potential breach. Review events and action taken and alter procedures accordingly.

*Computer System Security.* Under 201 MCR 17.04, businesses that “electronically stores or transmits [personal information] must also establish and maintain a security system covering its computers, including any wireless system.

The plan must include: securing user authentication protocols and access control measures; encryption of transmitted records and files containing personal information; the monitoring of networks and systems for unauthorized use or access of personal information; the review of audit trails and specific security measures for systems connected to the Internet; the use of current system security agents; a written policy regarding the restriction of access to personal information and how it is restricted; and the education and training of employees on all policies. Additionally, after any breach or potential breach, the integrity of records must be reviewed.



## In Conclusion

This rule contains a variety of very specific requirements and policies that all employers of Massachusetts residents (or businesses who own, store, license or maintain personal information of Massachusetts residents) must develop and implement. However, businesses must be vigilant to follow through with any policies to ensure that they're being followed and to respond appropriately if they're not. This includes regular audits of both systems and operations, technology and people. Employee non-compliance must be taken seriously, and businesses must communicate the importance of these policies to their people. The key will be not only to ensure that protections are in place, but to ensure an appropriate response if those protections fail.

For more information, please see the text of the General Laws of Massachusetts, Chapter 93H, the text of regulation 201 Massachusetts Code of Regulations ("MCR") 17, et seq.: Standards for the Protection of Personal Information of Residents of the Commonwealth, or the website of the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR).

**The Devine, Millimet & Branch Labor, Employment and Employee Benefits Group offers this free Friday E-Mail Alert service to provide information on recent developments in labor, employment and employee benefits law. If you have any questions about this e-mail, or if you know of anyone else who may be interested in receiving these alerts, please send us an e-mail at [employment@devinemillimet.com](mailto:employment@devinemillimet.com).**

"This is not a legal document nor is it intended to serve as legal advice or a legal opinion. Devine, Millimet & Branch, P.A. makes no representations that this is a complete or final description or procedure that would ensure legal compliance and does not intend that any reader should rely on it as such."

