

Deadlines for Massachusetts Personal Information Security Standards Extended

by Michael J. Cavaretta

In September the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) issued standards for protecting and storing the personal information of Massachusetts residents. These standards will apply to all businesses that store the “personal information” of Massachusetts residents, regardless of whether or not such businesses are located in Massachusetts. This new regulation will have a significant impact on Massachusetts employers, as almost all employers store “personal information” concerning their employees such as social security numbers, driver’s license numbers and financial account information.

Recognizing that the majority of breaches involve the theft of portable devices and that data encryption significantly neutralizes risk if information is lost or stolen, the OCABR regulations call on businesses to, among other things, encrypt documents sent over the Internet or saved on laptops or flash drives, encrypt wirelessly transmitted data, and utilize up-to-date firewall protection that creates an electronic gatekeeper between the data and the outside world and only permits authorized users to access or transmit data. The regulations also require businesses to ensure that third-party service providers are capable of adequately protecting personal

The standards will apply to all businesses that store the personal information of Massachusetts residents.

information, to contractually bind the third parties to do so, and to require the third parties to provide written certification of adequate protection. This will mean employers will have to review and modify service agreements for a variety of vendors that have access to employee information, including benefit plan administrators and payroll services.

These regulations were initially set to take effect on January 1, 2009, but citing “intervening economic circumstances,” the OCABR has extended the deadlines.

The new deadlines are as follows:

- ✓ The general compliance deadline has been extended from January 1, 2009 to May 1, 2009. The date is consistent with a new FTC Red Flag Rule, which requires financial institutions and creditors to develop and implement written identity theft prevention programs. Businesses addressing the new FTC requirements can now address the state regulations in the same time frame.
- ✓ The deadline for ensuring that third-party service providers are capable of protecting personal information and

contractually binding them to do so will be extended from January 1, 2009 to May 1, 2009, and the deadline for requiring written certification from third-party providers will be further extended to January 1, 2010.

- ✓ The deadline for ensuring encryption of laptops will be extended from January 1, 2009 to May 1, 2009, and the deadline for ensuring encryption of other portable devices will be further extended to January 1, 2010. According to the OCABR, many data breaches reported to date relate to laptops, and laptops are more easily encrypted than other portable devices such as memory sticks, DVDs and PDAs.

For additional information, please contact Mike Cavaretta at mcavaretta@mbbp.com.

The Morse, Barnes-Brown & Pendleton, PC, **Employment & Immigration Practice Group** provides sophisticated legal services and practical advice to employers of all sizes, ranging from technology start-ups to Fortune 1000 companies.

Robert M. Shea – rshea@mbbp.com

Mark H. Burak – mburak@mbbp.com

Donald W. Parker – dparker@mbbp.com

John J. Gallini – jgallini@mbbp.com

Scott J. Connolly – sconnolly@mbbp.com

Employment Law Advisor is intended as an information source for clients and friends of MBBP. It should not be construed as legal advice, and readers should not act upon information in this article without professional counsel.

© 2008 Morse, Barnes-Brown & Pendleton, P.C.

 **MORSE
BARNES-BROWN
PENDLETON** PC
The law firm built for business.®