HUNTON& WILLIAMS

CLIENT ALERT

September 2008

Contacts

Lisa J. Sotto
200 Park Avenue
New York, NY 10166
(212) 309-1223
lsotto@hunton.com

Elizabeth H. Johnson
One Bank of America Plaza
Suite 1400
421 Fayetteville Street
Raleigh, NC 27601
(919) 899-3073
ehjohnson@hunton.com

Additional Lawyers
Cédric Burton
James A. Harvey
Jörg Hladjk
Natalie Hunt
Christopher Kuner
Ryan P. Logan
Manuel E. Maisog
Melinda McLellan
Randall S. Parks
Olivier Proust
Boris Segalis
Aaron P. Simpson
Rachel M. St. John
Bridget C. Treacy
Mason Weisz
John W. Woods, Jr.

Centre for Information Policy Leadership
Martin E. Abrams*
Paula J. Bruening
Fred H. Cate
Orson Swindle*

*Not a lawyer

New Massachusetts Rules Require Strict Information Security Standards

Massachusetts recently issued regulations requiring any person who holds personal information about Massachusetts residents to develop and implement a comprehensive, written information security program to protect the data. The rules apply to both consumer and employee information, and require the protection of personal data in both paper and electronic formats. The deadline for compliance with the new requirements is January 1, 2009.

Scope of Coverage

The regulations apply to "every person" that "owns, licenses, stores or maintains personal information." "Person" is defined broadly to include natural persons, corporations and other legal entities. "Personal information" is defined as a Massachusetts resident's first and last name, or first initial and last name, *in combination with* his or her: (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 financial account. Personal information does not include data that are publicly available. As indicated above, the standards require safeguards for personal information maintained in either paper or electronic records. Consequently, the regulations apply to all private entities, regardless of size or industry sector, that hold personal information about Massachusetts residents in any media.

Requirements

Businesses with Massachusetts consumers or employees are now required to develop and implement a "comprehensive, written information security program." Organizations covered by the rules must limit the amount of personal information they collect to that necessary to accomplish the legitimate purpose for which the data are collected. They also must limit the time the information is retained to that reasonably necessary to accomplish the purpose of the collection, and must restrict access to those individuals who are reasonably required to know the information to accomplish that purpose or comply with records retention laws. The rules establish minimum standards to safeguard personal information, including:

- designating an employee to manage the written security program, implementing training programs and imposing disciplinary measures for employees who violate the program's requirements;
- identifying all records, systems and storage media, including laptops and portable devices, containing personal information (except where all records and storage devices will be treated as if they contain such information);

- assessing internal and external security risks and the effectiveness of current safeguards, and upgrading safeguards as necessary;
- instituting security policies that address employee access to records containing personal information and the transport of those records outside business premises;
- restricting physical access to records containing personal information; securing the records and data in locked facilities, storage areas or containers; and implementing a written procedure that sets forth the manner in which physical access to the records is restricted;
- regularly monitoring employee access to personal information;
- reviewing 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, and taking corrective action when indicated by the review process; and
- documenting actions taken in response to security breaches, with a mandatory post-incident review of events and actions taken, if any, to make changes in business practices.

Under the new rules, businesses must take reasonable steps to verify that service providers are capable of protecting personal information, and are required to contractually bind them to do so. In addition, organizations must obtain written certifications from their service providers confirming that the service providers have implemented a written information security program that complies with the regulations.

Encryption and Other Technical Requirements

Information Security programs implemented pursuant to the new standards must provide for encryption of electronic transmissions of personal information conducted wirelessly or across public networks. Businesses that store or transmit personal information electronically also must:

- establish user authentication protocols that include control of user IDs and a secure method of assigning passwords (including prohibiting use of vendor-supplied default passwords);
- maintain reasonably up-to-date operating system security patches, firewalls, anti-malware programs and virus definitions;
- ensure that password location does not compromise the security of the data it protects, restrict access to active users only and block access after multiple unsuccessful attempts; and
- engage in periodic system monitoring for signs of unauthorized use or access.

Significance of the New Rules

The regulations impose exceptionally stringent and comprehensive data security standards on all businesses with Massachusetts consumers or employees. Previously, similarly strict standards were applicable only to financial institutions and health care entities. The Massachusetts rules are the first in the nation to have such comprehensive and broad coverage applicable to all types of organizations.

The Massachusetts regulations resemble the Safeguards Rule promulgated pursuant to the Gramm-Leach-Bliley Act. But the new standards go well beyond the Safeguards Rule in both their scope and the specificity of the mandated security measures. The "minimum necessary" concepts associated with the collection, access and retention of personal information are reminiscent of European data protection laws and the federal Health Insurance Portability and Accountability Act's Privacy and Security Rules.

Massachusetts is now the second state in the U.S. to require encryption for the transmission of sensitive personal information. As described in a recent Hunton & Williams' Client Alert, beginning October 1, 2008, Nevada will require businesses in that state to encrypt customer personal information if those data are transmitted electronically outside the organization's "secure system."

We Can Help

Several states now require businesses that maintain personal information to implement data security measures. Hunton & Williams' Privacy and Information Management practice assists clients in developing, implementing and evaluating privacy and information security programs to comply with federal and state requirements. If you would like assistance in reviewing your organization's privacy or data security practices, or developing new policies or training programs, please contact us.