Paul Hastings
StayCurrent
A CLIENT ALERT FROM PAUL HASTINGS
January 2009

Massachusetts Imposes Far-Reaching Obligations to Protect Personal Information of its Residents

BY BEHNAM DAYANIM AND KELLY DEMARCHIS

Individuals and businesses that collect personal information have become accustomed to dealing with a web of state and federal laws. In addition to federal rules that regulate personal information, over 40 states currently have laws in place that require notice of the inadvertent disclosure of personally identifying information related to each individual state's residents.

For a long time, **California** has been the trendsetter in this area of the law, enacting a welter of laws intended to address data privacy and security concerns. Now, **Massachusetts** has gone one step further. New regulations require any person that owns, licenses, stores or maintains personal information in electronic form from Massachusetts residents to implement a "**written, comprehensive information security program**."[1]

"**Personal information**" is defined as a Massachusetts resident's first name or initial and last name, in combination with one of the following other pieces of information: (1) social security number; (2) driver's license number or state-issued identification number; or (3) financial account, credit card or debit card number.

Only entities that **electronically** store or transmit personal information are required to implement a plan. The new rules require the plan to be "reasonably consistent with industry standards" and to contain "administrative, technical, and physical safeguards" designed to ensure the security and confidentiality of the relevant records.

Most provisions of the new rules were originally scheduled to take effect on January 1, 2009, but since have been extended until **May 1, 2009.**

Amazingly, the new rules seem to have attracted little notice, perhaps lost in the general bedlam that accompanied the 2008 presidential elections and economic meltdown. However, with the compliance deadline looming, expect these requirements to garner a lot of comment – and to generate much activity – in the months ahead.

Procedural Component to the Rules

While individual plans are to be evaluated based on the size, scope and type of entity, its resources, the amount of data it stores, and its need for confidentiality and security, the new regulations require that each plan, **at a minimum**:

- designate one or more employees to maintain the program;
- identify records and storage systems that include personal information;

- identify and assess reasonably foreseeable risks to the security and confidentiality of the records containing personal information and evaluate and improve (where appropriate) the efficacy of current safeguards;
- develop security policies and training for employees;
- impose disciplinary measures for violations of the program;
- prevent terminated employees from accessing records containing personal information;
- take reasonable steps to verify that third-party service providers have the capacity to protect personal information and contractually require them to comply with the rules;
- limit the amount of personal information collected and retained to that reasonably necessary to accomplish its intended purpose;
- limit access to those persons who reasonably require it in order to accomplish the intended purpose;
- impose reasonable restrictions upon physical access to records containing personal information;
- regularly monitor to ensure that the plan is operating properly;
- review the scope of the security measures at least annually; and
- document responsive actions taken in connection with any incident involving a breach of security.

Technical Requirements

The new regulations also mandate certain minimum **technical** requirements, including:

- secure user authentication protocols, such as control of user IDs, reasonably secure methods of assigning and selecting passwords, control of data security passwords, restriction of access to active users only, and freezing of access after multiple unsuccessful log-in attempts;
- secure access control measures that restrict access on a need-to-know basis and assign unique identifications and passwords;
- encryption of transmitted records and files containing personal information;
- reasonable monitoring of systems;
- encryption of all personal information stored on laptops and portable devices;
- reasonably up-to-date firewall protection and operating system security patches; and
- reasonably up-to-date versions of system security agent software.

What to Do?

Absent court challenge or further regulatory action, these rules are set to take effect in May. How businesses respond will be of great interest.

The list of requirements appears daunting, but generally tracks the safeguards that businesses subject to existing federal data security regulatory requirements – such as financial institutions and health-care providers – already must have in place. For those businesses and others that already have implemented similar information security procedures, complying with the Massachusetts regulations may entail only a careful review of existing policies and practices and perhaps compilation or summary of existing procedures in a single document.

Nonetheless, the impact of the rules should not be minimized. **Any business that collects personal information of Massachusetts residents must comply with these provisions**. Third-party service providers also must comply. Persons subject to the rules must obtain written certifications from those service providers that they adhere to the rules in order to allow the providers access to Massachusetts personal information. The deadline for obtaining those certifications is January 1, 2010.

Entities that fail to comply with the regulations may be subject to enforcement action from the Massachusetts Attorney General's office. How vigorously the rules are enforced is an open question, but some businesses – presently blissfully unaware of the existence of these rules – may be in for an unwelcome surprise once they take effect.

The lesson here may be that while it pays to keep an eye on Sacramento, industries concerned with additional mandates in the data privacy and security fields should not forget our other state capitals, including, it would seem, Boston.

✧ ✧ ✧

Paul Hastings' Privacy and Information Security Practice advises clients on all aspects of privacy and information security law and regulation, conducts privacy assessments, formulates and helps establish privacy and security compliance programs, and represents clients facing state or federal privacy enforcement investigations or litigation. We also represent clients in working with Congress and regulatory agencies in the formulation and implementation of public policy in this dynamic and important area. Behnam Dayanim is a partner and Kelly DeMarchis is an associate in Paul Hastings' Washington, D.C., office.

For more information on the subject of this alert or on any other privacy or information-security related topic, please contact Behn or Kelly.

Washington, D.C.

Behnam Dayanim
202-551-1737
bdayanim@paulhastings.com

Kelly DeMarchis
202-551-1828
kellydemarchis@paulhastings.com

1 201 Mass. Code Regs. 17.03 – 17.04 (2008).

18 Offices Worldwide Paul, Hastings, Janofsky & Walker LLP www.paulhastings.com

Stay*Current* is published solely for the interests of friends and clients of Paul, Hastings, Janofsky & Walker LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2008 Paul, Hastings, Janofsky & Walker LLP.

IRS Circular 230 Disclosure: As required by U.S. Treasury Regulations governing tax practice, you are hereby advised that any written tax advice contained herein or attached was not written or intended to be used (and cannot be used) by any taxpayer for the purpose of avoiding penalties that may be imposed under the U.S. Internal Revenue Code.