



January 2009

**PRIVACY & INFORMATION
SECURITY UPDATE****New State Laws Increase Data Security Requirements**

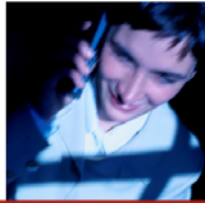
Identity theft and fraud are growing threats to both consumers and businesses and, not surprisingly, they have become top regulatory and law enforcement priorities. As part of this increased focus, commercial data security practices have come under increasing scrutiny. In addition to federal (and even international) regulatory initiatives, states have begun to set required standards for the secure storage and transmission of data by enacting legislation. For example, recently enacted laws in Massachusetts and Nevada set heightened standards for the protection of personal information. While presumably well-intentioned, these state-by-state responses add to the compliance burdens of affected businesses and may even create inconsistent and conflicting data protection standards. Nevertheless, for the time being, they are the law.

MASSACHUSETTS LAW

The new Massachusetts legislation goes into effect on May 1, 2009 and establishes “minimum standards” for safeguarding personal information stored in any medium, including electronic and paper records. The legislation applies to all entities that own, license, store or maintain personal information about a resident of Massachusetts, regardless of whether the entity operates in the state. “Personal information” is defined as first name (or first initial) and last name in conjunction with a Social Security number; a driver’s license or state-issued ID card number; or a financial account, credit or debit card number, with or without security or access codes. Those entities affected by the new legislation must “develop, implement, maintain and monitor a comprehensive written information security program applicable to any records containing such personal information.” The law provides a list of elements that must be included in the written information security program and describes computer system security requirements for electronic storage or transmission of personal information.

NEVADA LAW

A new Nevada data security law that went into effect on October 1, 2008 restricts the electronic transmission of personal information. All companies that conduct business in Nevada need to evaluate their current data security procedures to verify compliance with the requirements. This particular legislation is not limited to personal information of Nevada residents; transmission of any individual’s personal information is restricted. The new legislation requires businesses to encrypt all electronic transmissions, other than facsimiles, of personal information of a “customer” to a person “outside the secure system of the business.” Several of the terms require interpretation; for example, it is unclear what constitutes a “business in [Nevada].” In other



contexts, courts have considered the nature and quantity of in-state business to determine whether a company was doing business in Nevada. In addition, the new law does not specifically include a penalty for noncompliance, nor does it specify the agency responsible for enforcement. Noncompliance may open the door to civil suits for negligence.

THOMPSON HINE IS AVAILABLE TO ASSIST YOU

Thompson Hine's Privacy and Information Security practice, an interdisciplinary and international group of lawyers with experience in complex national and international issues including privacy, data protection, information security, records retention, employment and labor law, consumer protection, Internet law and intellectual property, can help you develop, implement and benefit from globally compliant data management practices. Our team has assisted numerous companies in developing and implementing global privacy and data protection programs and strengthening their strategic use of competitively critical data.

FOR MORE INFORMATION

If you would like more information on the Massachusetts or Nevada data security laws, please contact:

Thomas F. Zych	216.566.5605	Tom.Zych@ThompsonHine.com
Joanne E. Clifford	216.566.5758	Jodi.Clifford@ThompsonHine.com

If you do not wish to receive future communications by email, please reply to this email with "unsubscribe" in the subject line.

This advisory may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgement of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions. Some of the design images and photographs in this document may be of actors depicting fictional scenes.

© 2009 THOMPSON HINE LLP. ALL RIGHTS RESERVED.