

**THOMPSON
HINE**

April 2009

**PRIVACY & INFORMATION
SECURITY UPDATE****Identity Theft Compliance Deadlines Approaching**

We previously have reported on new and significant state and federal data security laws that may impose substantial compliance burdens on businesses. The compliance deadlines for those laws are rapidly approaching and it is important that businesses take steps to determine whether the laws apply to them and, if so, what they need to do to comply.

RED FLAG RULES ENFORCEMENT EFFECTIVE MAY 1, 2009

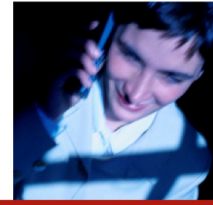
We previously reported that the Federal Trade Commission (FTC) has enacted rules, colorfully called the “Red Flag Rules,” that are aimed at reducing identity theft. The FTC delayed enforcement of the rules until May 1, 2009, due to confusion over their scope and applicability. This new compliance deadline is fast approaching. Financial institutions and businesses that extend or arrange for consumer credit that are subject to the rules should, if they are not currently in compliance with the Red Flag requirements, promptly develop and implement a comprehensive, written identity theft prevention program in order to avoid the penalties for noncompliance.

The Red Flag Rules apply to “financial institutions” and “creditors” that offer or maintain “covered accounts.” Under the rules, these terms are very broadly defined and include entities that in the past have not been required to comply with similar FTC rules in other contexts. Consequently, even enterprises that have not previously been under the mandates of the FTC’s data security rules should immediately evaluate whether Red Flag compliance is required and respond accordingly. If covered, each financial institution and creditor must develop a written identity theft prevention program that identifies and detects the relevant warning signs or “red flags” of identity theft. The program must be in effect on or before the May 1, 2009 deadline.

For more information on the Red Flag Rules, go to
www.ThompsonHine.com/publications/pdf/2008/10/privacyinformation1554.pdf.

MASSACHUSETTS DATA SECURITY REQUIREMENTS EFFECTIVE JANUARY 1, 2010

In response to financial challenges brought about by the current economic conditions, the Massachusetts Office of Consumer Affairs and Business Regulations (OCABR) extended the mandatory compliance date for its new data security law to January 1, 2010. Enforcement was originally scheduled to begin on January 1, 2009; however, the deadline was pushed back to provide greater flexibility in fostering compliance. Under the new law, all persons who “own, license, store, or maintain personal information about a resident” of Massachusetts are required to “develop, implement, maintain and monitor a comprehensive *written* information security program applicable



to any records containing such personal information.” This requirement is not limited to parties that are conducting business in Massachusetts and will affect all entities that store personal information about Massachusetts residents. Covered parties may be required to take data security measures as extensive as full encryption of the covered data, as well as other specified compliance measures.

NEVADA DATA SECURITY REQUIREMENTS ALREADY IN EFFECT

Beginning October 1, 2008, a new Nevada data security law went into effect that increases restrictions on electronic transmissions of personal information. Under the new law, all companies that conduct business in Nevada are required to encrypt “electronic transmissions” of “personal information of a customer” to a person “outside the secure system of the business.” The law does not define or limit what nexus a company must have to Nevada in order to be conducting business in the state. Consequently, the full breadth of the law’s reach remains to be seen, and companies that operate on a nationwide basis should evaluate whether their existing data transmission policies comply and respond accordingly.

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 these data security laws, please contact:

Thomas F. Zych	216.566.5605	Tom.Zych@ThompsonHine.com
Michelle W. Cohen	202.263.4151	Michelle.Cohen@ThompsonHine.com
Carolyn S. Flahive	614.469.3294	Carolyn.Flahive@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.