



May 2009

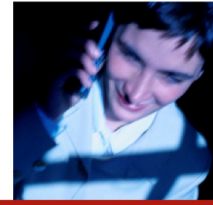
**PRIVACY & INFORMATION
SECURITY UPDATE****Compliance Deadline for Identity Theft Rules Delayed Again****FTC RED FLAGS ENFORCEMENT EFFECTIVE AUGUST 1, 2009**

The Federal Trade Commission (FTC) again has suspended its enforcement of the new “Red Flags Rules” until August 1, 2009, due to ongoing Congressional debate over the appropriate reach and scope of the rules. As we previously reported, the rules broadly mandate the adoption and use of identity theft policies and procedures by financial institutions as well as companies that provide or arrange for the extension of consumer credit. The Red Flags Rules originally were scheduled to take effect on November 1, 2008, but the deadline has been pushed back several times as a result of pervasive confusion over the scope and applicability of the rules. The latest deadline of May 1, 2009 has been pushed back to August 1 of this year.

The Red Flags Rules require each financial institution or “creditor” to develop a written identity theft prevention program that identifies and detects relevant warning signs, or “red flags,” of identity theft. The term “creditor” is broadly defined and covers more than just banks and other lenders. Consequently, entities that are not generally required to comply with FTC rules in other contexts are subject to the Red Flags Rules. The required identity theft prevention program must be comprehensive and designed to detect, prevent and mitigate potential data exposure following a “red flag” event. The program must be managed by a board of directors or senior employees and must include appropriate staff training. Further, covered entities must oversee service provider arrangements. A “service provider” is defined broadly as “a person that provides a service directly to the financial institution or creditor.” A covered entity cannot escape its obligations to comply with the final rule by simply outsourcing an activity.

Specifically, whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts, the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

The FTC expects industries and associations to use this additional time to “to share guidance with their members” to ensure that all covered entities are compliant by the new enforcement deadline. Thus, despite the extension, all covered entities should continue working diligently to develop a written identity theft prevention program that will be ready to deploy by August 1, 2009.



To aid in compliance, the FTC has prepared a guidebook for navigating the scope and requirements of the Red Flags Rules, currently available on its web site: <http://www.ftc.gov/redflagsrule>. In addition, the FTC plans to release a template to assist entities with a low risk of identity theft to develop a compliant identity theft program. The template will also be available on the FTC web site.

As a reminder, although the FTC has suspended enforcement, the Department of the Treasury, Federal Reserve System, Federal Deposit Insurance Corporation and National Credit Union Administration continue to adhere to the original November 1, 2008 compliance deadline. As such, all entities regulated by these federal agencies should already be compliant with the red flags requirements or risk the penalties of noncompliance.

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

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 Red Flags Rules, please contact:

Thomas F. Zych	216.566.5605	Tom.Zych@ThompsonHine.com
Michelle W. Cohen	202.263.4151	Michelle.Cohen@ThompsonHine.com
Joanne E. Clifford	216.566.5758	Jodi.Clifford@ThompsonHine.com
Carolyn S. Flahive	614.469.3294	Carolyn.Flahive@ThompsonHine.com
Darcy Brosky	216.566.5774	Darcy.Brosky@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.