

Last Minute Reprieve: FTC Gives Businesses Until August 1, 2009 to Adopt Identity Theft Prevention Programs To Comply With Federal Red Flags Rules

Written by Colin J. Zick

May 1, 2009

On Thursday, April 30, 2009, just 24 hours before the Federal Trade Commission (FTC) was set to begin enforcement of federal Red Flags Rules, the FTC [announced](#) that it was giving businesses three additional months, until August 1, 2009, to comply with the new identity theft regulations. The FTC also promises to provide a “template” for compliance directed to “entities that have a low risk of identity theft.” This announcement is welcome news for businesses that have been struggling to develop a compliant program by the end of the day today.

The FTC, FDIC and other federal regulatory authorities adopted the Red Flags Rules in January 2008 in response to the enactment of the Fair and Accurate Credit Transactions Act, 15 U.S.C. § 1681. The Rules have been in effect for banks, credit card companies and traditional financial institutions since November 1, 2008. However, there have been delays in enforcement of the broadest of the Red Flags Rules, as set forth in 16 C.F.R. Part 681, which apply to “creditors.” In 2008, the FTC caused considerable controversy when it announced that it was construing the term “creditor” to apply to any business that sells goods or services now and bills its customers later, including doctors, lawyers and many other businesses. As a result of this broad interpretation, confusion about who should be complying with the Red Flags Rules has been pervasive across many industries, especially the healthcare industry. Acknowledging this confusion, the FTC repeatedly postponed the original November 1, 2008 deadline for businesses swept into the FTC definition of “creditor.”

In general, the Rules require that a “creditor” perform a routine self-assessment to determine whether it maintains any kind of account that creates a reasonably foreseeable risk of identity theft. This would include a consumer account maintained by a utility company or cell phone provider, any other account that permits multiple customer transactions or a wide range of other “covered accounts.”

If your business offers or maintains “covered accounts,” it must develop a written identity theft prevention program to detect the warning signs or “Red Flags” of identity theft and mitigate the potential harm caused to consumers. The basic elements of a compliant identity theft prevention program include:

- The appointment of a identity theft / information security coordinator;
- Procedures to identify Red Flags, warning signs and security risks;
- Procedures for responding to Red Flags that have been detected;
- An effective training program to educate staff on how to recognize and respond to Red Flags; and
- Ongoing oversight and monitoring of the identity theft prevention program.

The FTC announcement indicates that it will release a “template” for businesses that have a low risk of identity theft, “such as businesses that know their customers personally.” According to the FTC, the August 1, 2009 deadline should give “low-risk” businesses an opportunity to use the FTC template to develop a compliant program. At this stage, it is unclear how helpful the upcoming template will be for most businesses. Anyone affected by the Red Flags Rules should be taking reasonable steps now to ensure that they are in a position to comply with the FTC regulations by August.

Author: Gabriel M. Helmer

This communication is intended for general information purposes and as a service to clients and friends of Foley Hoag LLP. This communication should not be construed as legal advice or a legal opinion on any specific facts or circumstances, and does not create an attorney-client relationship.

United States Treasury Regulations require us to disclose the following: Any tax advice included in this document was not intended or written to be used, and it cannot be used, for the purpose of avoiding penalties under the Internal Revenue Code.

Attorney advertising. Prior results do not guarantee a similar outcome. © 2017 Foley Hoag LLP. All rights reserved.