

# Red Flags Rule



## Can the “Clarification Act” be any less clear?

On December 18, 2010, the President signed into law the "Red Flag Program Clarification Act of 2010," which clarifies the type of "creditor" that must comply with the Red Flags Rule and specifically outlines that this rule should not be applied to physicians generally.

The new law indicates that creditors who fall under the Red Flags Rule are only those who regularly and in the ordinary course of business: (1) obtain or use consumer reports, directly or indirectly, in connection with a credit transaction; (2) furnish information to certain consumer reporting agencies in connection with a credit transaction; or (3) advance funds to or on behalf of a person, based on the person's obligation to repay the funds or on repayment from specific property pledged by them or on their behalf (this does not include creditors who advance funds on behalf of a person for expenses incidental to a service provided by the creditor to that person). Creditors that fall under one or more of the above-mentioned categories must comply with the Red Flags Rule by December 31, 2010. Creditors that do not fall under one of these categories are not subject to the Red Flags Rule. The FTC has not yet voiced its opinion to the act, but it is anticipated that there will be an appeal to the ruling filed in the near future.

## Whats your Risk Tolerance?

Although the language in this new ACT does not appear to be completely clear, it is the opinion of many legal professionals that it was the intent of the legislation to exempt hospitals as well as physicians. So the question becomes, “What is your Risk Tolerance”? Even if the new “clarity” exempts mandates and potential fines, It does not make the private information in physician practices or Hospitals immune to (medical) identity theft and other related identity theft prevention laws. Medical identity theft is on the rise and with new Healthcare reform looming around the corner, and with electronic storage/distribution models being the primary focus, there is no doubt that the identity theft trend will continue to grow. Although it’s uplifting and encouraging to watch governmental bodies gnash teeth, fight, and sue one another (kidding) over who should and shouldn’t be subject to the requirements, most of us in the risk management world don’t understand what the big dispute is. These programs are easy to find and simple to administer within an organization. There are even many programs and resources that can be found at no cost. An Identity Theft Program is a good business practice and just makes good business sense. Regardless of where your counsel guides you, having an identity theft prevention program in place is not only smart but also highly recommended. Protect your patients' information from misuse regardless of if you are forced into it or not and in the end you will be glad you did.

\*\*\*Jason Lavender is the Founder of Austin based ID Theft Solutions of America [www.idtsoa.com](http://www.idtsoa.com) . He is a Certified Identity Theft Risk Management Specialist (CITRMS) and has been featured as an expert in corporate identity theft prevention and related programs for many publications, news outlets, as well as state and federal law enforcement agencies. He can be contacted at [Jlavender@idtsoa.com](mailto:Jlavender@idtsoa.com) or 512-814-0200.