

### FTC Red Flags Rule: Are You in Compliance?

April 2009

As of May 1, 2009, the Federal Trade Commission (FTC) will begin enforcing the so-called "Red Flags Rule" issued jointly by the FTC, the federal bank regulatory agencies and the National Credit Union Administration (NCUA). The Red Flags Rule (the "Rule"), which went into effect on January 1, 2008, requires financial institutions and creditors to implement written Identity Theft Prevention Programs designed to prevent, detect and mitigate the damage of identity theft in their day-to-day operations. Although the FTC delayed its enforcement of the Rule until May 1, 2009, other agencies (which generally do not have enforcement authority over health care providers) retained enforcement authority as of the original compliance date of November 1, 2008.

Are you a Creditor?

Under the Rule, a "creditor" includes "any entity that regularly extends, renews, or continues credit." Since September of 2008, the American Medical Association (AMA), the Medical Group Management Association (MGMA), and other medical professional associations have been in dialogue with the FTC over whether the definition of "creditor" under the Red Flags Rule properly encompasses physicians and other health care providers. Although health care providers may not generally consider themselves creditors, the FTC has taken a contrary position with respect to the Rule. Specifically, the FTC has maintained the position that physicians and other health care providers are "creditors" when they regularly defer payment for goods or services. As such, physicians and other health care providers who regularly bill patients for services rendered, rather than requiring payment up-front, are considered creditors for purposes of compliance with the Red Flags Rule. As managed care plans and government health programs typically prohibit the practice of requiring payment up front for the provision of medical services, physicians and other health care providers generally will not be able to avoid application of the Rules by demanding payment in full up front.

Do you Have Covered Accounts?

Only those financial institutions and creditors with "covered accounts" are required to implement a written Identity Theft Prevention Program. For purposes of the Rule, "covered accounts" can take two forms: (i) an account offered or maintained primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions; or (ii) any other account offered or maintained for which there is a reasonably foreseeable risk (to customers or the financial institution or creditor) from identity theft. FTC attorneys have taken the position that covered accounts include continuing relationships with consumers for the provision of medical services.

Are you Required to Implement a Written Identity Theft Prevention Program?

Hospitals, physician practices, and other health care providers need to analyze their operations to determine whether they are required to comply with the Rule. In designing and implementing an Identity Theft Prevention Program ("Program"), as necessary, providers need to be cognizant of the

four Program elements required under the Rule. The Program must include reasonable policies and procedures to: (i) identify relevant red flags for the covered accounts and incorporate those red flags into the Program; (ii) detect red flags that have been incorporated into the Program; (iii) respond appropriately to any red flags that are detected in order to prevent and mitigate identity theft; and (iv) ensure the Program is updated periodically to reflect changes in risks (to customers and the financial institution or creditor) from identity theft.

Through existing compliance efforts, health care providers may already be in partial compliance with the requirements of the Rule. Whether or not this is so, providers who find they are subject to the Rule should be mindful of the impact the requisite Identity Theft Prevention Program may have on compliance with existing regulations, such as HIPAA.

*Billee Lightvoet Ward is an attorney in the Kalamazoo and Grand Rapids offices of Miller Canfield. She represents physician practices, hospitals and other health care providers in health law and corporate matters. She assists her clients in the drafting and implementation of policies and procedures and other documents necessary for the operation of their business, drafts and negotiates contracts of all types, and provides counsel on regulatory matters relating to EMTALA, fraud and abuse, federal and state confidentiality laws, corporate practice of medicine, and other compliance issues. If you have questions about the Rule, or need assistance with your compliance efforts, please contact Ms. Ward at 269.383.5860 or ward@millercanfield.com.*