



# Health Law Alert

Legal and political developments  
affecting the health care industry

A publication of Nixon Peabody LLP

OCTOBER 2008

## FTC “Red Flag Rules” effective November 1, 2008

*By Rebecca Simone and Michele Masucci*

On November 9, 2007, the Federal Trade Commission (FTC), National Credit Union Administration, and federal bank regulatory agencies jointly issued regulations known as the “Red Flag Rules,” implementing sections 114 and 315 of the Fair and Accurate Credit Transaction Act of 2003 (72 Fed. Reg. 63718). The purpose of the Red Flag Rules is to require financial institutions and creditors to address the risks or “red flags” of identity theft and implement a compliant Identity Theft Prevention Program. The rules may affect certain health care entities, and compliance is required by November 1, 2008. Penalties for non-compliance with the Red Flag Rules may include civil monetary fines and enforcement actions.

### To whom do the Red Flag Rules apply?

The Red Flag Rules apply to all financial institutions or “creditors” that offer or maintain one or more “covered accounts.” Various health care entities will fall under the rules’ broad definition of “creditor,” and many are likely to have patient accounts that would be considered covered accounts under the rules. A **creditor is defined as any entity that regularly accepts deferred payments for its goods or services and a covered account is** (1) an account primarily for personal, family, or household purposes **that involves or is designed to permit multiple payments or transactions**, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft.

The guidelines included in the final publication of the Red Flag Rules include specific mention of the health care industry: “For instance, creditors in the health care field may be at risk of medical identity theft (i.e., identity theft for purpose of obtaining medical services) and, therefore must identify Red Flags that reflect this risk.” (72 Fed Reg 63727). Additionally, in a July FTC business alert, the FTC stated that “[w]here non-profit government entities defer payment for goods or services, they too, are to be considered creditors.” An example of a health care scenario that would be covered by the Red Flag Rules would be a provider of health care services who regularly allows patients to defer payments and maintains accounts into which multiple payments are accepted from patients.

## What do the Red Flag Rules require?

Creditors that are subject to the Red Flag Rules must periodically determine whether they offer or maintain covered accounts. Creditors that offer or maintain more than one covered account must develop and maintain a board-approved written Identity Theft Prevention Program by November 1, 2008. The program must be designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account, and must be appropriate to the size and complexity of the creditor and the nature and scope of its activities.

Although the Red Flag Rules do not include specific text to be included in a program, they do include some requirements for the program's establishment and administration:

1. The program must be in writing;
2. The program must include reasonable policies and procedures to: (i) identify relevant Red Flags (defined as patterns, practices, or specific activities that indicate the possible existence of identity theft) 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 to prevent and mitigate identity theft; and (iv) ensure the program is periodically updated to reflect changes in risks;
3. Approval of the initial program must be obtained from the creditor's board of directors or an appropriate committee of the board of directors;
4. Staff must be trained, as necessary, to effectively implement the program;
5. Appropriate and effective oversight of service provider arrangements must be exercised; and
6. Creditors must consider the Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation (Interagency Guidelines) and must include those guidelines in their programs that are appropriate.

For health care entities, as the guidelines indicate, programs will likely include policies and procedures for dealing with the threat of medical identity theft. The "service provider arrangements" that must be overseen by the creditor may include entities such as third-party billing companies. The Interagency Guidelines, which are issued as an appendix to the final rule, identify 26 Red Flags, including inconsistent personal identifying information and suspicious payment patterns on a covered account. Although the Interagency Guidelines must be considered, creditors (including health care entities) have the flexibility to establish programs that fit their size and complexity. **Compliance with the Red Flag Rules is required by November 1, 2008.**

If you have any questions or require further information, please contact Michele Masucci at [mmasucci@nixonpeabody.com](mailto:mmasucci@nixonpeabody.com) or 516-832-7573; Rebecca Simone at [rsimone@nixonpeabody.com](mailto:rsimone@nixonpeabody.com) or 516-832-7524; or any member of Nixon Peabody's Health Services Team.