On November 1, 2008, the FTC's "Red Flag" regulations go into effect and now, despite initial uncertainty, it has become clear that the FTC considers these rules applicable to hospitals and health care providers that provide services to patients without requiring those patients to pay in full at the time of service. Although the deadline is fast approaching, there are manageable steps providers and practitioners can take to be in compliance, or substantially on the road to compliance, by the deadline.

**Background**

The Red Flag regulations (16 C.F.R. pt. 681) require companies to "develop and implement a written Identity Theft Prevention Program ("Program") that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account." 16 C.F.R. § 681.2(d)(1). Red Flags are those events that the FTC says should alert an organization that there is risk of identity theft, e.g., the new patient fails to provide all required personal information; or a dormant patient account is suddenly very active. The FTC recently clarified that the Red Flag regulations apply to any entity that
functions as a "creditor," by allowing deferred payment for services that are utilized by an individual for personal, household or family purposes. Thus, any health care provider or practitioner that allows a patient to pay for services over time is now a "creditor" under these rules. As such, these organizations must comply with the regulations and develop a Program designed to protect against identity theft. Providers and practitioners must adopt a Red Flag compliance plan by November 1, 2008.

**What does this mean for health care providers and practitioners?**

Despite the looming deadline, designing the required compliance plan should not be daunting or difficult. To the contrary, unlike other covered entities, health care providers usually have personal interactions with the individual to whom they are providing services. Therefore, health care providers and practitioners are in a reasonable position to verify the patient's identity at the time of service via review of photo identification, for example. Thus, this simple step could be instrumental in preventing a hospital from billing an innocent third party who then must endure a collections process or who may suffer an impaired credit history.

In light of the lower risk for identity theft in the health care space, preparing a Program to comply with the Red Flag regulations should be a straightforward five-step process that can be accomplished without significantly disrupting a provider's current practices. These steps are outlined below.

**Step One: Identify**

The first step is for health care providers to "[i]dentify relevant Red Flags for the covered accounts that the ... creditor offers or maintains, and incorporate those Red Flags into its Program." 16 C.F.R. § 681.2(d)(2). This should include the following:

1. An assessment of the risk factors for identity theft, including:
   - the types of covered accounts it offers or maintains,
   - the methods it provides to start providing services to new patients, and
   - its previous experiences with identity theft.
2. A review of prior experiences with identity theft and any methods of identity theft prevention the health care provider has utilized to date. Thus, any current identity theft prevention policies and procedures already in place should be included in the Program and modified to address newly-identified Red Flags.
3. A defined goal. The plan should be designed to detect patterns and identify behavior that preceded previous reports of identity theft to ensure that the Program includes detection and escalation
procedures within the provider’s chain of command that will allow the provider to respond before identity theft occurs, or to minimize its effect if it does occur. This step is best accomplished by developing a working group of key hospital personnel who would have been involved in collections-related activities for contested bills, e.g., patient financial, IT and HIM representatives.

Step Two: Review Appendix

The FTC, in the Appendix to the Red Flag regulations, also provides a list of Red Flags that creditors should specifically consider, even if they have not necessarily had experience with them in the past. The following Red Flags from that list may be applicable to a hospital or health care provider:

- the presentation of suspicious documents or personal identifying information, such as a suspicious address change;
- the unusual use of, or other suspicious activity related to, a covered account; and
- notice from customers, victims of identity theft and law enforcement that identity theft may have occurred.

The correct Red Flags usually can be identified through a working group involving, for example, Admissions Director, Billing Office Administrator, IT Administrator, and New Patient Intake Manager.

Step Three: Triggers

After reviewing its own experience (Step 1) and the Appendix (Step 2), the health care provider should create a list of “triggers” or Red Flags that it will attempt to detect and when detected, take action to prevent identity theft. Those triggers are the focus of the remaining two steps: detection and escalation.

Step Four: Detection

The Program must include methods for detecting the identified triggers, or Red Flags, in connection with the opening of deferred payment or “covered accounts” and existing covered accounts. 16 C.F.R. § 681.2(d)(2)(ii); 16 C.F.R. § 681.2. Additionally, the detection methods outlined in the plan should specifically provide for means of “obtaining information about and verifying the identity of a person opening an account” and means for “authenticating customers, monitoring transactions, and verifying the validity of change of address requests.” Id. This detection requirement may be met simply by initiating a policy of checking a valid photo identification document, or other validation document, to confirm the person receiving the service, and
thus opening an account, is, in fact, the person to whom the hospital will submit the bill.

**Step Five: Escalation**

Once the provider identifies the triggers, it should implement a plan to "[r]espond appropriately to any Red Flags that are detected." 16 C.F.R. § 681.2(d)(2)(iii). Thus, a provider must have a process in place to escalate triggers it has detected to employees that can take action to prevent or limit identity theft. The Appendix provides some examples of appropriate responses in non-health care settings which can be adapted for the health care environment.

**Implementation: Approving, Reporting, and Updating**

Once the health care provider has finalized its Program, it must present it to its Board of Directors, or a sub-committee thereof, for approval. 16 C.F.R. § 681.2(e)(1). Following Board approval, the health care provider must train staff and put in place methods for supervising any service providers that may access covered customer accounts — such as billing or collection agencies. 16 C.F.R. § 681.2(e)(3) & (4). This training, education and monitoring feature may be folded into the provider's existing, broader corporate compliance program related to its health care and other activities. The Board must then continue to exercise oversight over the development, implementation, and administration of the program. 16 C.F.R. § 681.2(e)(2).

Finally, a provider must report to its Board of Directors on at least an annual basis regarding the identified incidents and effectiveness of the Program. Appendix at (b)(2). In other words, the Red Flag reports to the Board should address significant identity theft incidents, and recommendations for material changes in the Program. Id. As a part of overseeing the Program, any material changes made because of new information must be approved by the Board of Directors. 16 C.F.R. § 681.2(e)(2). Changes to the Program may be warranted based on new experiences with identify theft; changes in identity theft methods; changes in the methods to detect, prevent and mitigate identity theft; changes in the types of accounts offered; and new mergers, acquisitions, or alliances involving the health care provider. Id. at V.

For more information about the subject matter of this e-Alert, please contact your regular Sonnenschein attorney.

To register for this and other Sonnenschein publications, please visit http://www.sonnenschein.com/misc/signup.html.
To unsubscribe from the Health Care publications list, please click here.

These materials should not be considered as, or as a substitute for, legal advice and they are not intended to nor do they create an attorney-client relationship. Because the materials included here are general, they may not apply to your individual legal or factual circumstances. You should not take (or refrain from taking) any action based on the information you obtain from this document without first obtaining professional counsel and you should not send us confidential information without first speaking to one of our attorneys and receiving explicit authorization to do so.

This e-mail was sent by Sonnenschein Nath & Rosenthal LLP, located at 1301 K Street, N.W., Suite 600, East Tower, Washington, D.C. 20005-3364 in the USA.

Health Care Group
Sonnenschein Nath & Rosenthal LLP
www.sonnenschein.com