International Hearing Society
16880 Middlebelt Rd., Ste. 4 ● Livonia, MI 48154
p 734.522.7200 ● f 734.522.0200
www.ihsinfo.org

IHS Member Advisory
Is Your Practice Compliant with the Federal Trade Commission Red Flags Rule?

As many as nine million Americans have their identities stolen each year. In an effort to curb the incidence of this crime, the Federal Trade Commission (FTC) issued a set of regulations known as the Red Flags Rule, which require certain businesses and organizations, including healthcare providers, to develop a written program to spot the warning signs or "red flags" of identity theft.

UPDATE: The enforcement of the Rule went into effect on January 1, 2011; however, questions have been raised about the applicability of the rule in light of passage of S.3987, "the Red Flag Program Clarification Act of 2010," signed into law on December 18, 2010. S.3987 exempts from compliance entities or individuals who advance funds on behalf of a person for expenses incidental to a service provided by the entity to that person. An example of "incidental to" would include attorneys who "advance funds on behalf" of their clients for expenses such as court filing fees and copy costs, which are repaid by the client at a later date. Since hearing aids would not likely be considered incidental to the service, hearing aid specialists who extend credit likely still need to comply with the Red Flags Rule. IHS encourages its members to review the Red Flags Rule website at www.ftc.gov/redflagsrule for more information, or seek counsel from your attorney if you are uncertain about the applicability of the Rule to your practice.

Who Must Comply

Every healthcare practice must review its billing and payment procedures to determine if it is covered by the Red Flags Rule. **Whether the law applies to you is not based on your status as a healthcare provider, but whether your activities fall within the law's definition of the term "creditor."** The definition of a "creditor," modified in December 2010 through S.3987, includes those individuals or entities that regularly:

- Obtain or use credit reports when determining credit transactions;
- Provide information to credit reporting agencies; or
- Advance funds to or on behalf of a person, based on an obligation of the person to repay the funds, or repayable from specific property pledged by or on behalf of the person.

In addition, the law applies to any other type of "creditor…as the agency…may determine appropriate…based on a determination that such creditor offers or maintains accounts that are subject to a reasonably foreseeable risk of identity theft." The definition of "reasonably foreseeable risk of identity theft" is expected to be clarified in subsequent rule-making by the FTC.

Spotting Red Flags

What red flags signal identity theft? There is not a standard checklist, but here are a few warning signs that are important to be aware of:

Suspicious documents. Has a new patient given you identification documents that look altered or forged? Is the photograph or physical description on the ID inconsistent with what the patient looks like? Under the Red Flags Rule, you may need to ask for additional information from that patient.

Suspicious personal identifying information. If a patient gives you information that does not match what you have learned from other sources, it may be a red flag of identity theft. For example, if the patient gives

International Hearing Society
16880 Middlebelt Rd., Ste. 4 ● Livonia, MI 48154
p 734.522.7200 ● f 734.522.0200
www.ihsinfo.org

you a home address, birth date, or Social Security number that does not match information on file, fraud could be present.

Suspicious activities. Is mail returned repeatedly as undeliverable, even though the patient still shows up for appointments? Does a patient complain about receiving a bill for a service that he or she did not get? These questionable activities may be red flags of identity theft.

Notices from victims of identity theft, law enforcement authorities, or others suggesting possible identity theft. Have you received word about identity theft from another source? Cooperation is key. Heed warnings from others that identity theft may be ongoing.

Setting Up an Identity Theft Prevention Program

The Red Flags Rule gives healthcare providers flexibility to implement a program that best suits the operation of their practice. If you are covered by the Rule, your program must identify the kinds of red flags that are relevant to your practice; explain your process for detecting them; describe how you will respond to red flags to prevent and mitigate identity theft; and spell out how you will keep your program current.

According to the Red Flags Rule, your program must be approved by your Board of Directors, or if your practice does not have a Board, by a senior employee. The Board or senior employee may oversee the administration of the program, including approving any important changes, or designate a senior employee to take on these duties. Your program should include information about training your staff and provide a way for you to monitor the work of your service providers — for example, those who manage your patient billing or debt collection operations. The key is to make sure that all members of your staff are familiar with the Rule and your new compliance procedures.

What is at Stake

Failure to comply with the Red Flags Rule could open a violator up to $3,500 per violation, civil liability for damages, and reasonable attorney fees sustained by the person injured in connection with the fraudulent activity. Compliance with the Red Flags Rule assures your patients that you are doing your part to fight identity theft.

The FTC has published "Fighting Fraud with the Red Flags Rule: A How-To Guide for Business," a handbook on developing an identity theft prevention program. For a free copy of the guide and for more information about compliance, visit www.ftc.gov/redflagsrule.