Red Flags Rule Protects Patients

FTC Rule on Identity Theft Impacts Providers

By David N. Anthony, Paige S. Fitzgerald, and Erin S. Whaley of Troutman Sanders LLP, Richmond, Va.

Identity theft is a significant and growing problem. According to a study released in February 2007, identity theft increased 50 percent from 2003 through 2006 with more than 15 million Americans victims of identity theft in 2006 alone. In response to these staggering figures and in an effort to prevent and combat this crime, the Federal Trade Commission (FTC) and other federal agencies issued regulations affecting financial institutions and creditors—common witnesses to identity theft.

The Red Flags Rule, issued November 2007, requires financial institutions and creditors to develop and implement written identity theft prevention programs in connection with the Fair and Accurate Credit Transactions (FACT) Act of 2003. These regulations necessitate the identification, detection, and response to patterns, practices, and specific activities indicating identity theft in a formal program.

Clear Up Any Confusion

Many health care providers have asked whether the Red Flags Rule applies to them. Not surprisingly, health care providers typically do not consider themselves financial institutions or creditors and do not generally fall under FTC rules. As a result, most providers paid little attention to the Red Flags Rule program's initial compliance implementation date of Nov. 1, 2008. Health care providers were not the only businesses with questions about the Red Flag Rule. A few days before the original compliance date, the FTC decided to delay enforcement of the Red Flags Rules for six months until May to give financial institutions and creditors additional time to develop and implement written programs.

The FTC's broad preliminary interpretation of "creditor" within the Red Flags Rule means any business offering services not paid in full at the time of the provision of services. This definition would expand coverage far beyond traditional lenders, such as banks, finance companies, mortgage brokers, automobile dealers, telecommunications companies, and utility businesses.

Health care providers clearly are not financial institutions, but many are creditors under the FTC's broad definition. The FTC explained "health care providers are creditors if they bill consumers after their services are completed" (www.ftc.gov/bcp/edu/pubs/articles/art11.shtm).

For instance, if a health care provider collects a co-payment at the time of service, submits a claim to the patient's insurance company, receives payment from the insurance company, and then bills the patient for any remaining amounts owed, the provider is a creditor under the Red Flags Rule. Similarly, if a provider allows patients to pay their accounts on a monthly basis, the provider is a creditor.

Given confusion on how the Red Flags Rule applies to health care providers and the potential steps to take and expenses to pay for compliance, the American Medical Association (AMA) and 27 other specialty medical organizations sent a detailed letter on Sept. 30, 2008 to the FTC chairman (www.ama-assn.org/ama1/pub/upload/mm/31/ftc_letter20080930.pdf). The AMA's letter objected to the FTC's Red Flags Rule applying to health care providers and asked for clarification. The FTC has not responded formally to the AMA's letter, and has not indicated intent to do so. Because the FTC's intention is unclear, health care providers should continue their efforts to comply with the Red Flags Rule by the May 1 deadline. If providers do not, they risk fines from the FTC of up to $2,500 per offense according to 15 U.S.C. § 1681s.

Take Steps to Comply

The Red Flags Rule outlines necessary and specific steps for providers to take to create an identity theft protection program for compliance. First, the provider should conduct a risk assessment to identify their vulnerabilities. The risk assessment should examine, among other things.

- the procedures the provider uses to open its accounts;
- the procedures the provider has for allowing access to accounts (such as password protections, etc);
- the provider's previous experience (or lack of experience) with identity theft; and
- identification of potential red flags.

A *red flag* is a pattern, practice, or specific activity indicating the possibility of identity theft. Typical medical identity theft warning signs concerning health care providers include:

- records showing medical treatment that is inconsistent with the patient's history;
- suspicious documents, such as a forged insurance card;
- a patient who has an insurance number but not a card or documentation; and
- unusual billing patterns.

After conducting an initial risk assessment, the Red Flags Rule requires health care providers to establish a formal, written identity theft program. Many health care providers may need to modify existing policies and procedures for protecting the privacy and security of health information. For instance, the Red Flags Rule requires health care providers to identify a "red flags manager." A health care provider may choose to expand the scope of a privacy, security, or compliance officer to include new red flags responsibilities instead of establishing an entirely new position.

The Red Flags Rule requires four basic elements to be present in an identity theft program. They are

- identify relevant red flags of identity theft and incorporate those into the program;
- detect of red flags in connection with the customer accounts;
- respond appropriately, commensurate with the degree of risk posed, to any red flags detected by the health care provider so identity theft will be mitigated and prevented; and
- ensure the program is updated periodically, taking into account changes in circumstances.

While an identity theft program must have these four elements, like the Health Insurance Portability and Accountability Act (HIPAA), the Red Flags Rule gives health care providers flexibility to design an appropriate identity theft prevention program for the provider's size, complexity, and unique circumstances.

Once the health care provider completes a risk assessment and finalizes a program, the provider's board of directors, an appropriate board's committee, or designated senior level manager must formally adopt the program. The provider must train staff to effectively implement the program and to periodically update the program. The Red Flags Rule also contains an explicit requirement that an annual report (or a more frequent report) be prepared for the board or a designated senior level management employee evaluating the effectiveness of the Red Flags program. The report should address identity theft risks when opening covered accounts and any significant identity theft incidents for existing covered accounts, management's response, and any recommendations for material changes to the program.

Target Medical Identity Theft

The Red Flags Rule may have other significance to health care providers besides identify theft to patient's financial accounts. Health care providers also need to be aware of medical identify theft, as issued in 72 Fed. Reg. 63,727 (Nov. 9, 2007). The consequences of theft and misuse of health care records can be as severe as the theft of an individual's financial records. Medical identity theft causes not only financial difficulties but has the potential to cause physical harm to its victims. Given the increasing economic and government pressure on health care providers to adopt electronic billing and medical records systems over the past decade, health care providers have become a target-rich environment for identify theft criminals. A health care provider's best practices should include instituting a program to guard against identity theft and protect the provider and patients.

The Red Flags Rule requires creditors to develop an identity theft prevention program tailored to their unique situation. Given the rule's requirements and the penalties for noncompliance, health care providers are advised to contact an attorney to assist with Red Flags Rule compliance requirements by the May 1, 2009 deadline.

David Anthony is a partner in the Consumer Law and Complex Litigation Practice Groups of Troutman Sanders LLP. He regularly represents businesses in consumer and commercial litigation and compliance issues. (david.anthony@troutmansanders.com)

Erin S. Whaley is an associate with Troutman Sanders LLP, where she has practiced since 2004. She practices health care law and advises health care providers on a broad range of issues, including regulatory compliance. (erin.whaley@troutmansanders.com)

Paige S. Fitzgerald has been an associate with Troutman Sanders LLP since 2004. She is a member of the consumer law and health care practice groups, and regularly counsels clients in numerous regulatory compliance areas. Before joining Troutman Sanders, Paige served as an assistant attorney general at the Virginia Attorney General's office and was counsel to Virginia's Medicaid agency. (paige.fitzgerald@troutmansanders.com)