Red Flags Rule In Limbo: Controversy Keeps Enforcement at Bay

Save to myBoK

By Chris Dimick

Lawsuits, lobbying, and legislation are holding up enforcement of the Federal Trade Commission's identity theft prevention law.

The Red Flags Rule has been all bark and no bite since the federal regulation was published in November 2007. More than two years and four postponements later, the Federal Trade Commission has yet to begin enforcing the identity theft prevention law.

The rule requires healthcare providers and others to develop, implement, and monitor identity theft prevention programs. But lobbying, lawsuits, and an act of Congress have postponed the rule's enforcement. The opposition and the delays have many in healthcare wondering what has become of the Red Flags Rule and whether small healthcare providers will remain covered by its requirements.

The Beginning: 2003

The rule originated in the Fair and Accurate Credit Transactions Act of 2003, which required financial institutions and any institutions considered "creditors" to maintain identity theft prevention programs. These programs would help identify, detect, and respond to patterns or activities-known as red flags-that may indicate identity theft.

Development and enforcement of the rule was given to the Federal Trade Commission, and in November 2007 the FTC published a final rule that indicated financial institutions were not the only entities covered by the rule. Healthcare providers as well as attorneys and other businesses were also covered, the FTC determined, because they provide a service or good and then bill after the fact or in installments. These billing practices make them a "creditor" under the rule, according to the FTC.

Originally, enforcement of the rule was to begin in November 2008. But the FTC had a long fight ahead of it before enforcement could begin, one that continues today.

Delays and Lobbying

Resistance to the rule centered on two charges: that the rule lacked clarity and that the FTC overreached its charge and applied it to too many types of businesses.

The backlash began with complaints that the FTC provided inadequate guidance on what businesses are considered creditors under the rule, according to Chris Apgar, CISSP, president of Apgar and Associates, based in Portland, OR. Apgar, a healthcare consultant, has written and presented on the Red Flags Rule.

"It is rather vague," Apgar says. "I can look at this rule and still walk away not really knowing who is covered by it and who isn't covered."

Many in healthcare did not learn they were covered by the rule until just months before the original enforcement date, causing professional associations to take up arms. Outcry from powerful groups like the American Medical Association and the American Bar Association began to flood the FTC and Congress.

In several letters to the FTC, the AMA wrote that providers had no warning the rule applied to them and needed time to prepare. It felt the FTC should republish the rule and allow providers to comment. The FTC contends that it has been clear that healthcare providers were covered since the rule was published in November 2007. It points out that medical identity theft is mentioned in the preamble.

However, the FTC did agree to postpone enforcement to May 2009 in order to provide more guidance. The new enforcement date did not hold, either, as medical and legal groups continued to contest their inclusion and cite a lack of guidance.

Enforcement of the rule would get pushed back a total of four times. The FTC created a Red Flags Rule Web site, conducted seminars and conferences for compliance training, and helped trade associations develop model policies for their members to use in creating their medical identity theft prevention programs.

While some groups continue to pressure the FTC to change its definition of creditor, healthcare experts following the rule say they feel the FTC will stick to its original interpretation of the law. Apgar notes that the commission has not given in to the pressure so far.

Disagreement on Who Is a Creditor

The FTC, at the direction of Congress, based its definition of "creditor" on the Equal Credit Opportunity Act (ECOA), which was passed by Congress in 1974 to eliminate discrimination by creditors against credit applicants on the basis of sex or marital status. The law was created with respect to all aspects of credit transactions.

A creditor under that act is "any individual who regularly extends, renews or continues credit; or any person who regularly arranges for the extension, renewal or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit."

In drawing up the Red Flags Rule, the FTC determined that industry groups like healthcare providers, attorneys, and accountants were all creditors under the ECOA definition. ECOA was written for any business that offers services on credit, and the Red Flags Rule, the FTC determined, should follow suit.

The ABA, AMA, and others objected. They insisted that their members should be exempt.

The AMA has argued in a letter to the FTC that practice physicians are not creditors under the ECOA definition because most do not "regularly extend, renew or continue credit." The AMA also says that the FTC overstepped its application of the Red Flags Rule to industries not originally intended by Congress. The Red Flags Rule was intended for financial institutions and other classic creditors, it wrote.

The AMA is not speaking publicly on the matter and refers media to letters it has written to the FTC.

Regardless of the lobbying, the FTC is unlikely to change its determination that healthcare providers are creditors under the rule, says Naomi Lefkovitz, an attorney with the Federal Trade Commission.

The FTC sticks by its analysis that service providers like physicians who offer a service upfront and accept payment later are indeed issuing credit to individuals-individuals who may be getting services under a false identity and then sticking their victims with the bill. This type of post-billing transaction, common in healthcare, is what identity thieves target, she says.

Lefkovitz believes it is important that healthcare providers be required to maintain identity theft prevention programs because healthcare is already a target of identity thieves. Based on a study conducted in February 2010, the Ponemon Institute estimates that nearly 1.5 million people have been victims of medical identity theft. Nearly half of those in the study had lost their health insurance as a result.

The theft can lead to more than the financial burden of resolving the billing issues or regaining insurance. When identity thieves seek medical care with a stolen identity, their medical information can become mixed into their victims' records. This can lead to dangerous medical results if the thief's information is later used to treat the victim.

House Bill Exempts Small Businesses

The most recent postponement of the Red Flags Rule came at the request of Congress. On October 30, 2009, the FTC announced that it was pushing back the November 1 enforcement date to June 1, 2010, in order to allow Congress time to consider a bill that dramatically alters Red Flags Rule legislation.

Ten days before the announcement, a bill sponsored by Rep. John Adler (D-NJ) had raced through the House. The bill would amend FACTA to exclude "any health care practice, accounting practice, or legal practice with 20 or fewer employees" from the Red Flags Rule.

The bill, HR 3763, also excludes any other business that the FTC determines knows all its customers or clients individually, only performs services in or around the residences of its customers, or has not experienced incidents of identity theft.

"The Federal Trade Commission went too far and went beyond the intent of Congress by considering non-financial, service related industries to be 'creditors'…" Adler said in a floor speech before the vote. The rule, he stated, "would force thousands of small businesses to comply with burdensome, expensive regulations by forcing them to develop and implement an identity theft program."

After swift unanimous passage of the amendment, the legislation was sent to the Senate and referred to the Committee on Banking, Housing and Urban Affairs, where it currently sits.

Will the Senate Follow?

The House amendment has raised its own objections.

Groups including AHIMA have spoken out against the exemption. Nearly half of all physicians work in practices of five physicians or fewer, AHIMA wrote the chair of the Senate committee, citing a 2008 report from the Center for Studying Health System Change. By exempting these smaller practices from the rule, the FTC would open up providers to potentially more medical identity theft at a time when such crimes are on the rise.

AHIMA argued that the risk to patients and the impact on healthcare fraud that result from medical identity theft far outweigh the requirements of the Red Flags Rule.

The threat of identity theft in physician offices and small healthcare practices is great enough that the country cannot afford to skip enforcement at that level, says Don Asmonga, director of government relations at AHIMA. Asmonga has represented AHIMA's opposition to the amendment to Congress.

The fate of the bill in the Senate and its impact on the FTC's enforcement timeline are uncertain. Asmonga believes the Senate Committee on Banking, House and Urban Affairs will not get to the bill before the FTC's June 1 enforcement deadline, if at all.

In addition, members of the committee have told Asmonga that even if they do get to HR 3763 during the current session, they would want to conduct their own fact-finding and legislative hearings. Several senators stated their concern for outright exempting any healthcare providers if it meant increasing the risk of medical identity theft.

Thus while the bill passed speedily in the House, its progress in the Senate will be much slower and its implications on medical identity theft considered more closely, Asmonga says. If the bill is not voted on before Congress adjourns in October, it would need to be reintroduced in the next session.

However, Apgar believes that the speed with which the bill passed the House, coupled with the powerful healthcare lobby groups backing it, give it a good shot at passing.

It is not clear what the FTC will do if the Senate does not act by June 1. The FTC has three options, Apgar suggests: postpone the enforcement date again in deference to Congress; begin enforcement despite Congress; or officially implement enforcement but delay any enforcement actions until HR 3763 is settled.

"I can't say at this point what our response would be," Lefkovitz, the FTC attorney, says.

If the Senate does not take up HR 3763 by June 1, Asmonga believes the FTC will start enforcement rather than delay it a fifth time.

It is the FTC's opinion that it does not have the authority to exempt certain industries from the rule, Lefkovitz says. It believes that exemptions have to come from Congress or the courts.

2007

November: FTC publishes final rule, requirements take effect

2008

November: Original enforcement deadline (postponed)

2009

May: Second enforcement deadline (postponed)
August: Third enforcement deadline (postponed)
October: House of Representatives passes bill exempting small legal, accounting, and healthcare practices
October: US District Court rules FTC may not apply rule to attorneys
November: Fourth enforcement deadline (postponed)
November: US District Court receives lawsuit to exempt accountants from rule

2010

February: FTC appeals US District Court ruling exempting attorneys
June: Current enforcement deadline

Court Rules FTC Overreached

Lawyers have already won exemption. On the same day in October that the FTC announced its most recent postponement, the US District Court for the District of Columbia ruled that the FTC could not apply the Red Flags Rule to attorneys. The lawsuit, filed by the American Bar Association, claimed that the FTC had overreached its authority when determining that attorneys were creditors under ECOA.

In its ruling, the court stated that the FTC inclusion of attorneys was "both plainly erroneous and inconsistent with the purpose underlying the enactment of the FACT Act."

"The Commission not only seeks to extend its regulatory power beyond that authorized by Congress, but it also untimely and arbitrarily selects monthly invoice billing as the activity it seeks to regulate," the court's opinion statement read.

The ruling did not escape the AMA's notice. In a January 29 letter to the FTC, the AMA and three other healthcare associations once again made their case for exemption, saying the recent court decision to exempt attorneys gave credence to their request.

"Apart from the technical legal analysis, moreover, we see no basis for concluding that Congress intended to have the Rule apply to LHCPs [licensed health care professionals] but not to lawyers," the letter stated. "Indeed, implementation of the Rule with respect to LHCPs but not to lawyers would be manifestly unfair and anomalous."

On November 10, 2009, the American Institute of Certified Public Accountants took the ABA's same argument in the same court. It filed a lawsuit against the FTC in US District Court asking that accountants also be exempt from the Red Flags Rule.

The FTC, however, is standing its ground. In February it filed a notice of appeal on the court's ruling in the ABA case. It is too early to tell what effect the lawsuits will have on healthcare, but given the FTC's stance, it seems likely that if the healthcare industry wants an exemption, it will have to sue for it.

How Big Is the Burden?

The AMA has argued that requiring healthcare providers to design, implement, and monitor a medical identity theft prevention program would "increase the costs of health care and would impose burdens on our members-with little, if any, benefit to the public," according to one AMA Congressional letter.

But complying with the rule does not necessarily require an expensive, large-scale effort, according to Apgar.

"Implementing the program is far simpler than people tend to make it out to be," he says.

The FTC offers guidance on how to develop a compliant program, and many of the steps mirror existing requirements of the HIPAA security rule.

For example, the Red Flags Rule requires that providers conduct a risk analysis, identifying activities that represent a potential act of medical identity theft. This risk analysis determines an organization's "red flags" for identity theft, such as a patient being admitted with a potentially altered identification card. Identifying the red flags allows the organization to monitor for those occurrences.

The HIPAA security rule already requires organizations to conduct a risk analysis, Apgar says. The existing risk analysis can be expanded to include risk of identity theft.

The rule also requires the creation of a security incident response team to investigate and mitigate possible medical identity theft. This response team also is already required by the HIPAA security rule, and providers can alter their existing policies to add the identity theft duties to the current security incident response team.

Required staff training on spotting red flags can be included in the annual privacy and security training that covered entities should already be conducting, Apgar says. Minimal additional training needs to be added for staff in areas like registration, where medical identity theft red flags will crop up.

Organizations with robust privacy and security programs may have all these pieces in place. They can develop an umbrella policy that connects existing processes and demonstrates they meet compliance with the Red Flags Rule.

Using the ECOA definition of a creditor to apply the Red Flags Rule is not a perfect fit, Lefkovitz admits. Just because an organization bills later does not mean they are offering up something of value to identity thieves. Some trades, like accountants, have argued this point.

But the FTC has said that by focusing on risk assessment, the Red Flags Rule allows organizations to design their identity theft programs to meet their particular situation. The burden in developing a compliant program is low even with small providers, since the rule "allows you to tailor your program to the complexity of your organization," Lefkovitz says.

Compliance Deadline Long Past

Though enforcement of the Red Flags Rule has been delayed to June, the actual compliance requirement has been in effect since the final rule was published in November 2007.

The rule "is in effect, and people should be adhering to it today," Apgar says. Organizations should not wait until June to see what happens with the enforcement of the rule.

In fact, healthcare organizations should have an identity theft prevention program, regardless of the rule's fate, Apgar says. If a facility becomes embroiled in a medical identity theft, the harm to its public reputation and the threat of personal lawsuits is much more detrimental than a fine from the FTC.

"As with HIPAA, your biggest threat is not the federal government, it is the attorneys," according to Apgar.

While the rule waits in limbo, Lefkovitz says one thing is absolute.

"That is one thing I can say with certainty-the Red Flags Rule has brought out some strong opinions."

Chris Dimick (chris.dimick@ahima.org) is staff writer for the *Journal of AHIMA*.

Article citation:
Dimick, Chris. "Red Flags Rule In Limbo: Controversy Keeps Enforcement at Bay" *Journal of AHIMA* 81, no.4 (April 2010): 22-25.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.