

## The “Red Flags” Rule Part II – Are you low-risk or high-risk?

Richard C. Stevens  
Martin, Pringle, Oliver, Wallace & Bauer LLP

In the Volume 59, Number 2, Summer 2009, issue of this publication, my colleague Lora Jennings introduced you to the Red Flag Rules (RFR) in her article titled “Health Care Providers and Identity Theft – Ensuring Compliance with the ‘Red Flags’ Rule.” Since then, the Federal Trade Commission (FTC) has postponed its enforcement of the Rule until November 1, 2009.

According to some commentators, this fourth delay in enforcement has been a result of pressure from business and professional organizations like the American Medical Association, and the American Bar Association. Regardless, at some point, whether it is in November or after another delay, the FTC will ultimately declare the rule to be enforceable (Congress would have to act if the RFR were to be abrogated). Consequently, we thought it best to build on the previous introduction to the RFR with some additional discussion.

As we previously stated, whether a particular healthcare provider is required to comply with the RFR depends on whether the provider’s activities qualify the provider as a “creditor” who maintains “covered accounts.” We also previously discussed the underlying definitions of “creditor” and “covered accounts.” While this article will not work through the underlying analysis based in the applicable Code of Federal Regulations (CFR), you would be well advised to discuss with counsel whether your practice runs in such a way that it might *not* be required to comply with the RFR. In the absence of assurances from your legal advisor that your practice can ignore the RFR, most writers now agree that it is highly unlikely that anything but an all-cash practice would be excused from the RFR obligations.

In part, I reach this conclusion because most successful practices will, at the very least, allow their patients to pay co-pays or patient responsibility amounts after a determination has been reached by their insurance providers—even if the practice does not allow traditional accounts receivable to accrue. Additionally, the final language in the definition of a covered account seemingly wraps up every new patient intake and account set-up scenario when it says that a covered account is “[a]ny . . . account . . . for which there is a reasonably foreseeable risk . . . from identity theft, including financial, operational, compliance, reputation, or litigation risks.<sup>1</sup>

When this language is viewed against the backdrop of headlines where individuals successfully use stolen credentials to obtain medical care,<sup>2</sup> and the never ending political activity

---

<sup>1</sup> 16 C.F.R. 681.2(b)(3)(i)-(ii).

<sup>2</sup> Diagnosis: Identity Theft, BUS. WEEK, Jan. 8, 2007, [http://www.businessweek.com/magazine/content/07\\_02/b4016041.htm](http://www.businessweek.com/magazine/content/07_02/b4016041.htm).

regarding health coverage, it is hard to imagine the FTC thinking that even a cash-only clinic is outside of the scope of the RFR.

Thus, it seems best for most organizations to resign themselves to the idea that they should at least evaluate what level of risk their entities are at for identity theft. If “level of risk” is new terminology for you in this discussion, that might be because it is buried in the comments by FTC staff regarding the time that organizations will have to dedicate to implementing RFR programs. Naturally, such a source is not the highest level of reliability, but the RFR legislation and the resulting regulations simply haven’t been around long enough to provide lawyers with anything to go on besides the type of guidance I am about to discuss.

In the Federal Register, the FTC has indicated that there are three broad levels of risk for entities that need to consider the RFR: (1) entities subject to a high risk of identity theft, (2) entities subject to a low risk of identity theft, but having consumer accounts that will require them to have a written Program, and (3) entities subject to a low risk of identity theft, but not having consumer accounts.<sup>3</sup> The significance of evaluating which one of these may apply to your organization is that the FTC has indicated that category two entities can likely utilize a streamlined program to comply with the RFR. So, that begs the question: what is your entity’s level of risk?

The FTC has said: “In general, high-risk entities may provide consumer financial services or other goods or services of value to identity thieves such as telecommunication services or goods that are easily convertible to cash, whereas low-risk entities may do business primarily with other businesses or provide non-financial services or goods that are not easily convertible to cash.”<sup>4</sup> Thus, because most family physicians do not offer cash-related services, but do allow patients to pay over time, it is reasonable to conclude that the streamlined RFR program might be acceptable: “Groups with a low risk for identity theft may have a more streamlined Program—for example, simply having a plan for how they’ll respond if they find out there has been an incident of identity theft involving their business.”<sup>5</sup>

All of this would be of little consolation to those tasked with trying to implement an acceptable RFR program but for the FTC’s recent posting of “Red Flags for Low Risk Businesses” on its web site.<sup>6</sup> This document is essentially a template document for creating a low-risk RFR program. It still follows the four basic steps we told you about in the previous article:

1. Identify relevant red flags for the provider’s covered accounts;

---

<sup>3</sup> See 72 F.R. 63741.

<sup>4</sup> 72 F.R. 63741, FN 63.

<sup>5</sup> See <http://www.ftc.gov/redflagsrule>, FAQs.

<sup>6</sup> See [http://www.ftc.gov/bcp/edu/microsites/redflagsrule/RedFlags\\_forLowRiskBusinesses.pdf](http://www.ftc.gov/bcp/edu/microsites/redflagsrule/RedFlags_forLowRiskBusinesses.pdf).

2. Establish procedures to detect those red flags in the provider's day-to-day operations;
3. Establish the responses to red flags to prevent and mitigate identity theft; and
4. Describe how the provider will keep its Program current and educate staff about the Program.<sup>7</sup>

Naturally, this article is not a substitute for obtaining independent counsel regarding the RFR or the specific level of risk of identity theft in your practice. You should also consult with counsel regarding reliance on the FTC commentary. But, generally, the risk-based discussion and guidance in the FTC publications should provide some relief for those low-risk entities dreading a large-scale attempt to comply with the RFR. Of course, it may still take more than the one hour allowance that the FTC recently opined would be involved in assembling the streamlined program.<sup>8</sup>

---

<sup>7</sup> Don't forget that the RFR requires that the Identity Theft Prevention Program be approved by the healthcare provider's board of directors or an appropriate senior level management employee, if the provider does not have a board of directors.

<sup>8</sup> The "FTC staff believes that it may have underestimated the time low-risk entities may need to initially apply the final rule to develop a Program. Thus, FTC staff has increased from 20 minutes to 1 hour its previously stated estimate for this activity." 72 F.R. 63742.