Health Care Organizations Are Covered By The FTC's 'Red Flags Rule'

Understandably, much of the health care industry seems to be unaware of a rule jointly promulgated by the Department of the Treasury, the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Federal Trade Commission pursuant to the federal Fair Credit Report Act of 2003. This joint rule contains "guidelines for financial institutions and creditors regarding identify theft with respect to their account holders and customers".[1] Deep within the 58-page notice of the final rule is the following mandate: "[C]reditors in the health care field may be at risk of medical identity theft (i.e., identity theft for the purpose of obtaining medical services) and, therefore, must identify Red Flags that reflect this risk".[2]

Thus, health care organizations are required to comply with the "Red Flags Rule". A "Red Flag" is defined as a "a pattern, practice, or specific activity that indicates the possible existence of identity theft".[3] In a series of letters exchanged between September 30, 2008 and March 11, 2009 (all available on the FTC's website), the American Medical Association and the Federal Trade Commission debated whether physicians are subject to the Red Flags Rule. The AMA -- which asserted that physicians are not subject to the rule -- relied in part on the "extensive HIPAA privacy and security requirements applicable to physicians with respect to patient information".[4] In response, the FTC asserted that "the Red Flags Rule generally complements rather than duplicates HIPAA data security requirements". According to the FTC, while HIPAA is designed to "protect[] individuals' health information from compromise and misuse", the Red Flags Rule is designed to "prevent[] or mitigat[e] the misuse of that information if it is compromised".[5] More broadly, the FTC justified application of the Red Flags Rule to the health care industry by asserting the prevalence of medical identity theft, noting that "[a] nationwide survey conducted for the FTC found that 4.5% of the 8.3 million victims of identity theft had experienced some form of medical identity theft, including the fraudulent use of their health insurance to obtain medical care or to obtain health insurance in their name".[6] Thus, the FTC's position seems to be that the Red Flags Rule applies not only to physicians but to all health care providers.

Confirming that the FTC's response to the AMA was not confined to the question of whether physicians (and physicians alone) are covered by the Red Flags Rule, the FTC has published on its website two "Articles for Business" that make clear the scope of the rule: *What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft* and *Compliance Tips for Companies Offering Services In and Around the Home* (the latter seems to apply to the home care sector). Absent a successful challenge to the application of the Red Flags Rule to health care organizations, it is now incumbent upon such organizations to consider what obligations, if any, they may have under the rule. The current deadline for compliance with the Red Flags Rule is August 1, 2009.[7]

The Threshold Inquiry Under the Red Flags Rule

The Red Flags Rule directs that: "Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts".[8] The FTC defines a "creditor" as a "business or organization" which "regularly . . . extend[s] . . . credit", and defines "credit" as "payment . . . made after the product was sold or the service was rendered". Any health care organization that accepts deferred payments -- such as a provider that agrees to bill private-pay patients after services are provided -- is considered a "creditor" under the Red Flags Rule. Moreover, according to the FTC, "[e]ven if you're a non-profit or government agency, you still may be a creditor if you accept deferred payments for goods or services".[9]

If the organization is a creditor, it next must determine whether it maintains "covered accounts". An "account" is a "continuing relationship established by a person [e.g., a patient] with a creditor [e.g., a provider] to obtain a product or service [e.g., health care] for personal, family, household or business purposes".[10] A "covered account" is an "account" that is either : (i) "designed to permit multiple payments or transactions"; or (ii) "for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the . . . creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks".[11] Unlike the vagaries of the second option, the first option is straight-forward. If a health care organization that is a creditor maintains a patient "account" that is "designed to permit multiple payments or transactions", it must comply with the mandates of the Red Flags Rule.[12] In the unlikely event that a health care organization that is a creditor determines that it does not maintain any "covered accounts", that determination must be revisited "periodically".[13]

Establishing an "Identity Theft Prevention Program" Under the Red Flags Rule

Under the Red Flags Rule, if a health care organization is a creditor that "offers or maintains one or more covered accounts", it is required to "develop and implement a written Identity Theft Prevention Program [a "Program"] that is designed to detect, prevent, and mitigate identity theft" in connection with such accounts.[14] The Red Flags Rule is sufficiently flexible to permit a health care organization to design a Program that complies with the rule without causing undue burden. The rule specifically states that "[t]he Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities".[15] Indeed, the commentary included in the Federal Register notice emphasizes that "the final rules are flexible, and allow smaller financial institutions and creditors to tailor their programs to their operations".[16] Under the plain terms of the rule, the creditor's "Program" must be committed to writing.[17]

A Program under the Red Flags Rule has four elements. Specifically:

> The Program must include reasonable policies and procedures to:
>
> (i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;
> (ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;
> (iii) Respond appropriately to any Red Flags that are detected . . . to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.[18]

The FTC also offers a set of "guidelines" that an entity is required to consider in developing a Program.[19]

Identifying Red Flags. The guidelines discuss five categories of Red Flags:

- Alerts, notifications, or other warnings received from consumer reporting agencies or services providers, such as fraud detection services.
- The presentation of suspicious documents.
- The presentation of suspicious personal identifying information, such as a suspicious address change.
- The unusual use of, or other suspicious activity related to, a covered account.
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

A health care organization should identify Red Flags by considering how each of these categories relates to the organization's operations. For example, a hospital might identify as a "Red Flag" any discrepancy between a patient's insurance card and other documents presented during admission.

Detecting Red Flags. A health care organization's Program for identifying Red Flags should be tailored to the organization's particular operations. Neither the rule nor the guidelines prescribe in detail the manner in which Red Flags are likely to be detected. In the example above, the hospital might consider implementing a policy requesting certain accepted forms of identification for the purpose of verifying that the patient is indeed the individual whose name appears on the insurance card.

Preventing and Mitigating Identity Theft. Designing a program that includes preventing and mitigating identity theft presents particular challenges in the health care industry. While the FTC guidance suggest the temporary or permanent cessation of services when a Red Flag is detected, health care providers must also consider their legal and ethical obligations to provide patient care.

Periodically Updating the Program. The rule does not specify the frequency with which an entity is required to update its Program. However, the guidelines mention that the following circumstances warrant updating of a Program:

- The experiences of the creditor with identity theft.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent, and mitigate identity theft.
- Changes in the types of accounts that the creditor offers or maintains.
- Changes in the business arrangements of the creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Even outside these circumstances, however, a health care organization is required to update its Program "periodically".

Administration of an Identity Theft Prevention Program

Compliance with the Red Flags Rule also requires that a creditor's Program be approved by its board of directors (or an appropriate committee thereof).[20] Moreover, the entity must involve its board, an appropriate committee thereof, or a designated employee at the level of senior management "in the oversight, development, implementation, and administration of the Program", and staff must be trained "as necessary[] to effectively implement the Program".[21] To the extent the creditor outsources services in connection with any covered accounts, the rule and the guidelines require the creditor to exercise oversight over such arrangements. Thus, Program requirements should be incorporated into contracts with service providers.[22] While the Red Flags Rule does not specify any particular enforcement mechanisms, violations of the rule may lead to civil monetary penalties by the FTC.

FTC Resources for Compliance with the Red Flags Rule

The Red Flags Rule itself and related materials can be found on the FTC's website at http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml. This website includes a document entitled Fighting Fraud With The Red Flags Rule: A How-To Guide for Business (available at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf), which is a general overview of the Red Flags Rule from the FTC's perspective. For creditors that believe they are at low risk for identity theft, the FTC has created a document entitled *Complying with the Red Flags Rule: A Do-It-Yourself Prevention Program for Businesses and Organizations at Low Risk for Identity Theft* (available at http://www.ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm).

---

1 72 Fed. Reg. 63,718-01, 63,719 (Nov. 9, 2007).
2 *Id.* at 63,727.
3 16 C.F.R. § 681.1(b)(9). The Red Flags Rule itself, and a host of related material, can be found on the FTC's website at http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml.
4 Letter from Ms. Margaret Garikes to Hon. William E. Kovacic at 2 (9/30/09).
5 Letter from Ms. Eileen Harrington to Ms. Margaret Garikes at 8 (2/4/09) (hereinafter "Harrington Letter").
6 Harrington Letter at 3 (2/4/09).
7 The rule itself has been effective since January 1, 2008, but the FTC has twice delayed the date for enforcement, with the current deadline being August 1, 2009. The FTC's delayed enforcement date does not impact the schedule for enforcement by any of the other agencies which participated in the joint promulgation of the rule and have jurisdiction to enforce it, although such jurisdiction extends primarily to the financial services industry.
8 16 C.F.R. § 681.2(c).
9 Tiffany George and Pavneet Singh, The "Red Flags" Rule: Are You Complying With New Requirements For Fighting Identity Theft? (2008), http://www.ftc.gov/bcp/edu/pubs/articles/art10.shtm. This article also notes, however, that "simply accepting credit cards as a form of payment does not make you a creditor under the Rule".
10 16 C.F.R. § 681.1(b)(1).
11 16 C.F.R. § 681.1(b)(3).
12 As an employer, a health care organization may have compliance obligations under the Red Flags Rule with respect to 403(b) and 401(k) plans maintained for its employees. The FTC is expected to issue guidance in the form of "FAQs" concerning whether and under what circumstances such plans are deemed "covered accounts".
13 16 C.F.R. § 681.1(c).
14 16 C.F.R. § 681.1(d)(1).
15 *Id.*
16 72 Fed. Reg. 63,724, 63,719 (Nov. 9, 2007).
17 16 C.F.R. § 681.1(d)(1).
18 16 C.F.R. § 681.1(d)(2).
19 16 C.F.R. § 681.1(f).
20 16 C.F.R. § 681.1(e)(1). An entity without a board of directors must instead secure approval of the Program by "a designated employee at the level of senior management". 16 C.F.R. §681.2(b)(2)(ii).
21 16 C.F.R. § 681.1(e)(2),(3).
22 16 C.F.R. § 681.1(e)(4).

This *GT Alert* was prepared by **Matthew Fenster**. Questions about this information can be directed to:

- **Matthew Fenster** — 212.801.2155 (fensterm@gtlaw.com)
- Or your **Greenberg Traurig** attorney

Albany 518.689.1400	**Houston** 713.374.3500	**Philadelphia** 215.988.7800
Amsterdam + 31 20 301 7300	**Las Vegas** 702.792.3773	**Phoenix** 602.445.8000
Atlanta 678.553.2100	**Los Angeles** 310.586.7700	**Sacramento** 916.442.1111
Austin 512.320.7200	**London^** +44 20 8895 4060	**Shanghai** +86 21 6391 6633
Boston 617.310.6000	**Miami** 305.579.0500	**Silicon Valley** 650.328.8500
Chicago 312.456.8400	**New Jersey** 973.360.7900	**Tallahassee** 850.222.6891
Dallas 214.665.3600	**New York** 212.801.9200	**Tampa** 813.318.5700
Delaware 302.661.7000	**Orange County** 949.732.6500	**Tysons Corner** 703.749.1300
Denver 303.572.6500	**Orlando** 407.420.1000	**Washington, D.C.** 202.331.3100
Fort Lauderdale 954.765.0500	**Palm Beach County North** 561.650.7900	**White Plains** 914.286.2900
	Palm Beach County South 561.955.7600	**Zurich** + 41 44 224 22 44