

FTC’s Identity Theft Red Flag Rules – Applicable to Health Care Providers
John Alan Lewis and Todd Newton

INTRODUCTION - OVERVIEW

On November 9, 2007, the Federal Trade Commission (“FTC”), the Federal banking regulatory agencies, and the National Credit Union Administration, published a joint notice of final rulemaking in the Federal Register (72 FR 63718) finalizing the Identity Theft Red Flags regulations and guidelines. This rule, promulgated pursuant to the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”), requires financial institutions and creditors to develop and implement written “identity theft prevention programs” (the “Red Flag Rules”). The programs must be developed for the identification, detection, and response to patterns, practices, or specific activities – known as “red flags” – that could indicate identity theft. It is generally believed that health care providers fall under the definition of a “creditor.”

The final rule (16 C.F.R.§ 681.1, et seq.) became effective January 1, 2008, but full compliance with the rule, however, was not required until November 1, 2008. On October 22, 2008, the FTC announced its decision to delay enforcement of key elements of the Red Flag Rules until May 1, 2009. The delay will permit “creditors” and financial institutions subject to administrative enforcement of the Fair Credit Reporting Act by the FTC additional time to fully implement policies and procedures designed to thwart identity theft. The delay does not extend to the rule regarding address discrepancies (see following section) or to the rule regarding changes of address applicable to card issuers. However, the FTC’s current interpretation indicates that these rules apply to financial institutions as well as many entities in the health care industry.

The Red Flag Rules impact health care providers in at least two ways. First, anyone who uses “consumer reports” for insurance, employment, or credit purposes¹ is covered under the Red Flag Rules. Second, the Red Flag Rules will apply to health care providers in that it places obligations on “creditors and financial institutions”² to detect, prevent, and mitigate identity theft in relation to accounts covered under the Red Flag Rules. (See attached article from www.amednew.com)

I. USE OF CONSUMER REPORTS: VERIFICATION OF ADDRESSES

Consumer reports are used by many entities including health care providers (e.g. hospitals, physicians, nursing homes, and others (“Providers”)). The Red Flag Rules state that users of consumer reports must develop and implement *reasonable* policies and procedures to deal with address mismatches. These policies and procedures must allow the Provider to form a

¹ 16 U.S.C. 681.1(a)

² 16 U.S.C. 681.2(a)

“reasonable belief”³ as to whether the applicant is the person he or she claims to be. Also, users of the consumer reports who have a continuing relationship with the applicant and who regularly, in the ordinary course of business, furnish information to a consumer reporting agency from which they receive the report, must report a reasonably confirmed address to that agency when there is an address discrepancy. Bottom line, this portion of the Red Flag Rules requires a creditor to use reasonable diligence in reviewing applicants/patient information against the individual’s address on the consumer report. For the reasons set forth below, we believe the term “creditor” includes Providers.

II. IDENTITY THEFT – RED FLAG RULES

As noted above, the second portion of the Red Flag Rules requires any business that is a “creditor or financial institution”⁴ to have written processes and procedures in place to detect, prevent, and mitigate identity theft in relation to accounts covered under the regulations. While a Provider will not be considered a financial institution under the regulations, a Provider would be considered a creditor. Let’s dig down deeper and see why.

A. WHAT IS A “CREDITOR”?

The Red Flag Rules applies to any company that provides goods or services for personal, family, household, or business purposes without demanding immediate payment. The regulations include as an example telephone companies and utilities being creditors under this part of the regulation because they provide phone service, power, and water now, and send a bill later – at the end of the month.⁵ Under this analysis, a fair reading of this part of the Red Flag Rules would lead one to conclude that a Provider is a creditor since services are provided and payment is not made until after that date of service. While there are certainly times where the patient pays for services at the time of services rendered, most health care services involve multiple transactions in which payment is not made until after services are rendered.

It has been reported that certain professional organizations within the health care industry have requested a written explanation from the FTC as to the agency’s legal justification for concluding that physicians (or any other type of Provider) are creditors for purposes of these rules. It does not appear that the FTC has responded to this request, at least as of this date. It is the position of Mitchell Williams that a Provider will be deemed a “creditor” under the Red Flag Rules with respect to at least some, if not all the payment arrangements with patients. Accordingly, a Provider should plan to comply with the Red Flag Rules.

B. WHAT TYPE OF ACCOUNTS ARE COVERED UNDER THE RED FLAG RULES?

A creditor has a duty to protect against identity theft in connection with “covered accounts.” An “account”⁶ is a continuing relationship established by an individual to obtain a

³ 16 U.S.C. 681.1(c)

⁴ 16 U.S.C. 681.2(a)

⁵ 16 U.S.C. 681.2(a)(3)(i) and (5)

⁶ 16 U.S.C. 681.2(b)(1)

product or service for personal, family, or business purposes from a Provider. However, only “covered accounts” are addressed in the Red Flag Rules and there are two parts to the definition. First, a “covered account” is any account maintained by the Provider designed to cover multiple transactions or payments (“Covered Account(s)”). Second, a Covered Account is any account where there is a reasonable foreseeable risk to consumers or to the Provider’s safety and soundness “from identity theft, including financial, operational, compliance, reputation, or litigation risks.”⁷ The agreement of a Provider to provide services each month and accept payment afterwards creates the Covered Account. However, the Provider would also be maintaining a Covered Account if it holds an individual’s money as prepayment for services to be made.

Covered Accounts do not include bank accounts opened and maintained by a financial institution for an individual, even if a Provider is a signatory or has power as a guardian or conservator for the account. The entity that opens and maintains the account – the bank – has the obligations under the Red Flag Rules. In that situation the Provider’s duties are those set forth by contract and by fiduciary relationship.

The Red Flag Rules require each financial institution or creditor that offers or maintains one or more Covered Accounts to develop and implement a written Identity Theft Prevention Program (the “Program”). The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.⁸

III. DEVELOPING, IMPLEMENTING, AND ADMINISTERING IDENTITY THEFT PREVENTION PROGRAM.

Creditors are required under the Red Flag Rules to establish and maintain a comprehensive Identity Theft Prevention Program. While there is no specification as to the precise nature of the Program, the Provider must be able to demonstrate that it has established reasonable policies and procedures to “detect, prevent, and mitigate identity theft in connection with the opening of a Covered Account or any existing Covered Account.”⁹

A. IMPLEMENTATION OF THE PROGRAM.¹⁰

Overall responsibility and oversight of the Program rests with the financial institution or creditor’s board of directors, an appropriate committee of the board, or a designated employee at the level of senior management.¹¹ However, a good first step for a Provider would be to establish a risk assessment team. The team would assess potential risks for identity theft within the operations of the Provider. The Provider will be well served to see that the risk assessment team has representation from several different departments. While the assembly of a risk assessment team is not a regulatory requirement, it may prove useful from an operational

⁷ 16 U.S.C. 681.2(b)(3)(ii)

⁸ 16 U.S.C. 681.2(d)

⁹ 16 U.S.C. 681.2(d)

¹⁰ See generally Hutchings, Bond, and Loepere in ABA eSource October 2008 Volume 5 Number 2 for additional material on risk assessment terms.

¹¹ 16 U.S.C. 681.2(e)

perspective. The risk assessment team would perform the risk assessment procedures under the guidance and control of the Provider's Board of Directors or senior management team.

The risk assessment team and/or a Program should take several steps to develop and identify the identity theft including the following:

- Identify Covered Accounts. The risk assessment team should consider every way in which a would-be thief could take advantage of the Provider's relationship with its patients. This analysis would include the ways in which accounts are opened and the methods available to access an account.
- Identify Red Flags. A "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of identity theft. The activity should be taken from known threats. The Provider should include additional Red Flags from its own experiences with identity theft as well as applicable suggested Red Flags contained in the regulations.
- Assess the Risk Level. The team should consider the real life likelihood of a particular risk coming to pass. Some routes to identity theft are more likely than others.
- Determine the Appropriate Response. If the Red Flag is a suspicious medical billing on a Covered Account, an appropriate response may be to contact the entity or individual who performed the services to obtain more information. If the Red Flag is an address discrepancy, the response may be to ask for additional identification. The response will vary as appropriate to the risk level and the Red Flag detected.
- Document Results of the Risk Assessment. A well documented and thought out risk assessment process satisfies regulators and may potentially save money by avoiding security breaches and the costs of litigation and compliance issues.
- Prepare the Identity Theft Protection Program (the "Program"). The Program must be in writing. It should point to the specific policies that comprise the Program. Some policies and procedures may already be documented in existing Information Security protocols or matters or issues relating to HIPAA.
- The Program – More. The Program should include reasonable policies and procedures to:
 - Identify Red Flags;
 - Detect Red Flags incorporated into the Program;

- Designate appropriate responses to any detected Red Flags; and
- Ensure the Program is updated or reviewed periodically.
- **Require Board Approval.** The board of directors as well as designated members of senior management should review and must approve the Program. In addition, the Board must help, develop, implement, and oversee the Program. Oversight of the Program should include assigning responsibility for the Program's implementation and compliance, reviewing reports prepared by staff, training staff as necessary to effectively implement the Program, overseeing service Provider arrangements, and approving material changes to the Program. Approval by the Board should be obtained before the May 1, 2009 effective date.
- **Annual Reports - Updates.** The persons of staff who have a designated responsibility for the development, implementation, and administration of the Program should report to the Board-designated administrator at least annually regarding compliance with the Red Flag Rules. The annual reports should address items such as the policies and procedures of the Program, service provider arrangements, significant instances of identity theft, and the responses taken to the same, as well as recommendations for changes to the Program. The annual reports should be documented along with any changes that are adopted.
- **Assignment of Responsibility.** The person delegated by the Board or administration to have responsibility for the Program should take direct control of training employees and oversight of service Provider arrangements. This should be "line" responsibility with a definite reporting procedure.
- **Self Training.** Those members of staff who have open access to Covered Accounts must be trained as necessary regarding the policies and procedures that are applicable to a job function. The training should include hiring, refresher training as needed, and training on new policies and procedures when the Program is updated.
- **Review of Service Provider Arrangements.** Should a Provider engage other service providers to perform services in connection with one or more Covered Accounts (e.g. a billing agent, collection agent, or management company), the Provider must take steps to ensure that the service provider has reasonable policies in place to detect, prevent, and mitigate the risk of identity theft. This can be accomplished through a contract which would include the policies and procedures to detect relevant Red Flags that may arise in connection with the provision of services, and either report the Red Flags to the Provider or take appropriate steps to prevent, detect, and mitigate identity theft by setting up its own Program.

November 6, 2008

Page 6

Mitchell Williams will be glad to meet with management to discuss the impact of the Red Flag Rules on your organization. While the final implementation date for the Identity Theft Prevention Program has been delayed until May 1, 2009, it is clear that the FTC expects each creditor or financial institution to have a written Program in place on or before that date. For additional information, contact Alan Lewis at (479) 464-5656 or Todd Newton at (501) 688-8881.

JAL:dd