If you have any questions or would like additional information on the material covered in this *Alert*, please contact one of the authors:

Debra L. Hutchings
Associate, Chicago
+1 312 207 3884
dhutchings@reedsmith.com

Paul J. Bond
Associate, Princeton
+1 609 520 6393
pbond@reedsmith.com

Carol C. Loepere
Partner, Washington, D.C.
+1 202 414 9216
cloepere@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

FTC's Identity Theft Red Flag Regulations: Implications for Health Care Providers

In November 2007, the Federal Trade Commission ("FTC") issued sweeping regulations aimed at deterring, detecting and preventing identity theft. Under these rules, known as the Red Flag Regulations, 16 C.F.R. § 681.1 *et seq.* and Final Rule ("Red Flag Regulations"), financial institutions and creditors of covered accounts must establish a program to detect, prevent and mitigate identity theft. While somewhat unclear and perhaps counterintuitive, the breadth of the Red Flag Regulations and the FTC's current interpretation indicates that these rules apply to many participants in the health care industry. The rules become effective **November 1, 2008**.

The Red Flag Regulations have three parts, two of which pertain to the health care industry.* The first part applies to anyone who uses "consumer reports" for employment, insurance or credit purposes. The second part places obligations on "creditors and financial institutions" to detect, prevent and mitigate identity theft in relation to accounts covered under the Red Flag Regulations. This *Client Alert* addresses each part in turn.

Use of Consumer Reports: Verification of Addresses

Many health care providers, such as hospitals, physicians, nursing homes, assisted living facilities and others in the health care industry (collectively "Providers") use consumer reports to check for credit history and criminal backgrounds as part of the employment process, before offering services for which there is a delay in payment, or for admission purposes. The Red Flag Regulations require that users of consumer reports develop and implement reasonable policies and procedures to deal with an address mismatch. These policies and procedures must allow the Provider to form a "reasonable belief" as to whether the applicant is the person they claim to be. Additionally, users of consumer reports who have a continuing relationship with the applicant and who "regularly and in the ordinary course of business" furnish information to the consumer reporting agency from which they received the report, must report a reasonably confirmed address to that agency when there is an address discrepancy. As a practical matter, this rule requires reasonable diligence in reviewing applicants/patient information against the individual's address on the consumer report.

The Red Flag Identity Theft Program

The second part of the Red Flag Regulations require any business that is a "creditor or financial institution" to have written processes and procedures in place to detect, prevent and mitigate identity theft in relation to accounts covered under the regulations (the "Program"). While a Provider would not be considered a financial institution under the regulations, it is less clear whether a Provider would be considered a creditor.

Is a Provider a 'Creditor'?

We normally think of a creditor as someone like a mortgage lender or a credit card company that lends or advances funds. But, in fact, this second part of the Red Flag Regulations applies to any company that provides goods or services without demanding payment up front. To take one example from the FTC's commentary, telephone companies and utilities are "creditors" under this part of the regulations, because they provide phone service, power, and water *now*, and send a bill *later*—at the end of the month.

Our discussions with the FTC staff indicate that the agency views Providers as falling within the definition of creditors. This would apply to any Provider that provides services without

demanding payment at the time services are rendered. For example, suppose Mr. Smith is admitted to a hospital for surgery and post-operative care. The hospital bills Mr. Smith's insurance company for care, but is not actually paid by the insurer until after services are rendered. Under the Red Flag Regulations, the hospital is a creditor to Mr. Smith. Although there could be hospital services where the patient pays for the services at the time the service is rendered (*e.g.*, at a clinic or emergency department), most hospital services involve multiple transactions in which payment is not made until after services are rendered. In this way, the hospital is likely deemed a creditor under the Red Flag Regulations.

Consider another example. A nursing facility provides services to Ms. Garcia during the month of June, but prebills Medicaid in May, but receives payment in July. By means of that arrangement, the facility has become a creditor to Ms. Garcia within the meaning of the Red Flag Regulations, and subject to the regulation's requirements. Similarly, if an assisted living facility ("ALF") provides services to its residents and bills them at the end of the month, the ALF is a creditor to its residents. In sum, the FTC's position appears to be that use of invoices and delayed payment after the patient receives health care services creates a creditor relationship between the Provider and the patient for purposes of the Red Flag Regulations. The American Medical Association is reported to have requested a written explanation from the FTC of the agency's legal justification for concluding that physicians (or any other type of heath care provider) are creditors for purposes of these rules. No response from the FTC has been received to date. In the interim, based upon our communications with the regulators and the language of the regulations, we believe a Provider will be deemed a "creditor" under the Red Flag Regulations with respect to at least some, if not all, of its payment arrangements with patients, and therefore needs to comply with the new regulations.

What Kind of Accounts Are Covered Under the Regulations?

A creditor has a duty to protect against identity theft in connection with "Covered Accounts." An "account" is a continuing relationship established by an individual to obtain a product or service for personal, family or business purposes from a Provider. A Covered Account is any account offered or maintained by the Provider designed to cover multiple transactions or payments. A Covered Account is also any account where there is a reasonably foreseeable risk to consumers or to the Provider's safety and soundness "from identity theft, including financial, operational, compliance, reputation, or litigation risks." The agreement of a Provider to provide services each month and accept payment afterwards creates a Covered Account. However, the Provider would also be maintaining a Covered Account if it held onto 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 powers 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 Regulations. In that situation, the Provider's duties are those set forth by contract and by the fiduciary relationship.

Developing, Implementing and Administering the Identity Theft Program

As noted, under the Red Flag Regulations, creditors must establish a comprehensive identity theft prevention Program. While the regulations do not specify 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." The Program must be periodically updated to reflect changes in risks.

Before drafting the Program, a Provider may wish to consider assembling a team to perform a risk assessment. The Risk Assessment Team should include individuals from the different departments of the Provider involved in admitting residents, determining medical coverage, safeguarding information about residents, and billing for services (*e.g.*, the admissions department, the business office, the HIPAA Privacy Officer, and the like). Once assembled, the Risk Assessment Team should review how an individual's identity is verified when opening an account during admission, what information is gathered, how that information is stored, and

what steps could be taken to detect and prevent identity theft in connection with existing accounts.

Assembling a Risk Assessment Team is not a regulatory requirement. If one employee is well-versed in all aspects of a Provider's operation, that employee could perform the risk assessment with the involvement of the board of directors or senior management (required under the regulations). On balance, however, we believe the assessment would be most effective if the Provider (or the Provider's larger organization) draws from the experience of several departments.

Next, the Risk Assessment Team should take the following steps to develop the identify theft Program:

- ***Identify Covered Accounts*** – The Risk Assessment Team should identify and list the Covered Accounts. The Team should think of every way a would-be identity thief could take advantage of the Provider's relationship with its residents or patients.
- ***Identify Red Flags*** – A Provider's written Program should list identity theft Red Flags. A Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft. For example, the following are common Red Flags: presentation of documents that look to be forged, altered, or fake; a suspicious address change; and a resident demanding services or access to health records with unusual urgency or frequency. Of course, any warning from law enforcement or a consumer reporting agency that a resident may be an imposter should be taken seriously. A Provider should include additional Red Flags from its own experiences with identity theft, as well as the applicable suggested Red Flags contained in the regulations.
- ***Assess the Risk Level*** – When the Risk Assessment Team develops a list of the hypothetical ways that imposters could take advantage of the Provider's residents or patients, the Team should then consider the real-life likelihood of each particular risk coming to pass. Some routes to identity theft are more likely than others. A resident who is being admitted involuntarily is unlikely to be using someone else's identity. A resident or family member who is unusually active in demanding treatment or access to medical records may deserve a second look.
- ***Determine the Appropriate Response*** – Taking into consideration the relevant Red Flags the Provider has identified and the potential risk level for identity theft, including medical identity theft, the Team must then determine the appropriate response to those Red Flags. If the Red Flag is suspicious medical billing on a Covered Account, the 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*** – For compliance purposes, it is important for the Provider to document the results of the risk assessment. A well-documented and thought-out risk assessment process will help satisfy regulators and may potentially save money by avoiding security breaches, and costly litigation and compliance issues.
- ***Prepare the Identity Theft Program*** – The next step is to incorporate the findings from the risk assessment and prepare the written Program. Although some of the policies and procedures may already be documented in existing Information Security, HIPAA or other policies, it is a best practice to have a separate document that either sets out separately the Program, or points to the specific places in existing policies that comply with the Red Flag Regulations.
- ***Require Board Approval*** – The Board of Directors or a designated committee of the Board, or if no Board, then a designated employee at the level of senior management (collectively "Administrator"), must review and approve as well as help develop, implement and oversee the Program. Oversight of the Program includes 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 as appropriate, and approving material changes to the Program. Note that approval should be obtained *before* the November 1, 2008 effective date.

- ***Report Annually*** – Provider staff who has the designated responsibility of development, implementation, and administration of the Program must report to the Administrator at least annually regarding compliance with the Red Flag Regulations. The annual report should address such items as the policies and procedures of the Program, service provider arrangements, significant incidents of identity theft and the responses taken to same, as well as recommendations for material changes to the Program.
- ***Assign Responsibility*** – A great program of risk mitigation on paper is only worthwhile if someone actually implements it. The Administrator may delegate responsibilities but ultimately is responsible for overseeing the Program. For example, the Administrator may delegate responsibility for training employees to a designated person, and oversight of service provider arrangements to another.
- ***Train Staff*** – All staff who open and access Covered Accounts must be trained as necessary regarding the policies and procedures that are applicable to their job function. This would include training upon hiring, refresher training as needed, and training on new policies or procedures when the Program is updated.
- ***Review Service Provider Arrangements*** – If a Provider engages service providers to perform services in connection with Covered Accounts (*e.g.*, a billing 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 by requiring the provider via contract to have policies and procedures to detect relevant Red Flags that may arise in connection with the provision of services, and either to report the Red Flags to the Provider or take appropriate steps to prevent, detect and mitigate identity theft by setting up its own Program.

Given the November 1, 2008 effective date, health care companies should promptly take steps to establish their written identity theft program.

* * * * * *

* The third part pertains only to debit or credit card issuers. *See* 16 C.F.R. § 681.3.