Update on FTC's Identity Theft Red Flag Regulations: Address Discrepancy Rule and Identity Theft Prevention Rule as They Apply to Health Care Providers

If you have 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.

Client Alert 08-206

November 2008

reedsmith.com

This *Client Alert* updates information received from the Federal Trade Commission ("FTC") concerning application of its Address Discrepancy and Red Flag rules aimed at combating identity theft as they apply to health care providers and suppliers. As reported previously, these rules, collectively known as the Red Flag Regulations, 16 C.F.R. § 681.1 *et seq.* ("Red Flag Regulations"), apply to users of consumer reports and "creditors," which may include many participants in the health care industry.

Status of Enforcement: Delay on Red Flag Rule But Not on Address Discrepancy Rule

As reported previously on Oct. 22, 2008, the FTC issued an Enforcement Policy statement that delays enforcement of the Red Flags rule until May 1, 2009 (*http://www.ftc.gov/opa/2008/10/redflags.shtm*). This policy does not affect enforcement of the Address Discrepancy Rule, which became effective Nov. 1, 2008.

Address Discrepancy: Requirement to Verify Address Only Upon Receipt of a Notice of Address Discrepancy From a Consumer Reporting Agency

The Address Discrepancy portion of the Red Flag Regulations (16 C.F.R. §681.1) requires users of consumer reports to develop and implement reasonable policies and procedures to deal with an address mismatch. In our discussions with FTC staff members, they have clarified two aspects of this rule. First, the FTC is interpreting this requirement as only applying to consumer reports, also known as credit reports, issued by nationwide consumer reporting agencies ("CRAs"), as defined in Section 603(p) of the Fair Credit Reporting act ("FCRA"). Today, there are only three such nationwide CRAs: Esperian, TransUnion and Equifax. While the language of the Address Discrepancy rule is not expressly limited to the "big three," as a practical matter, consumer reports issued by these entities are the reports the FTC advised us it believes are currently subject to this rule.

Second, the FTC staff stressed that the obligation to conduct address verification only applies to a user of the consumer report that has received a "notice of address discrepancy" from one of the three nationwide CRAs. In other words, in the FTC staff's view, users of consumer reports, such as hospitals, nursing homes or other health care entities that may use consumer reports for employment or admissions purposes, are only technically required to perform the address verification upon receiving such an express "notice of address discrepancy." Organizations using consumer reports must have policies and procedures to allow them to form a "reasonable belief" as to whether the applicant is the person they claim to be upon receipt of such a notice. 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 CRA from which they received the report, must report a reasonably confirmed address to that agency when there is an address discrepancy. In practice, because the CRA's "notice of address discrepancy" might not be explicitly denominated as such—in fact, could simply be an asterisk by an individual's name—we believe it is still good practice for providers using consumer reports to exercise reasonable diligence in reviewing applicants/patient information against the individual's address on the consumer report.

Finally, as a reminder, this aspect of the Red Flag Regulations became effective Nov. 1, 2008 and is not subject to the FTC's delay in enforcement applicable to Red Flag Rules.

The Red Flag Identity Theft Program

The second part of the Red Flag Regulations (16 C.F.R. §681.2) 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"). As previously reported, the FTC has taken the position that if a provider furnishes services now and does not require payment at the time services are provided (or does not bill in advance), the provider is a creditor and must develop and implement an identify theft program.

Our discussions with the FTC staff confirm that a provider may have some relationships in which it is not a creditor. For example, if a facility requires all fees paid up front or at the time services are rendered, it is not a "creditor." However, if the facility has any private pay arrangements where the patient is not required to pay until after services are provided, or bills an insurance company at the end of a stay for services provided during the stay and is not actually paid by the insurer until after services are rendered, the provider is a "creditor." In practice, if a provider has any transactions in which it is a creditor, it then needs to look to determine whether it has any "covered accounts."

What Kind of Accounts Are Covered Under the Regulations?

A creditor has a duty to protect against identity theft in connection with "Covered Accounts." There are two types of "Covered Accounts": (1) an account that is a continuing relationship established by an individual to obtain a product or service for personal, family or business purposes designed to cover multiple transactions or payments; and (2) 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.

If a provider has either of these types of accounts, it is covered by the Red Flag Rule and must develop and adopt an identify theft prevention program.

Developing, Implementing and Administering the Identity Theft Program

FTC staff has made clear that the risk of identify theft—the "red flags"—associated with certain types of accounts will be greater than others. For example, the risk of someone using someone else's identify to obtain narcotics at a busy urban emergency department may be greater than the risk of someone being admitted to a small rural nursing home where many people in the community know one another. Therefore, providers should tailor their program to the risks presented by their operations. The FTC staff has stressed that the program should be risk-based and flexible.

The FTC staff has posted an article on its website to give health care providers guidance in the application of the rule (*http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm)*. Also, we understand the FTC will be issuing frequently asked questions and answers on the rule. Thus, as health care providers continue to develop and implement their identity theft programs in advance of the May 1, 2009 date, providers should check with FTC's website periodically for updated information.

Client Alert 08-206

November 2008

reedsmith.com