



HEALTH CARE ALERT

September 24, 2008

Are You “Red Flag Rule” Compliant?

As a result of Congressional amendments to the Fair and Accurate Credit Transactions Act, the Federal Trade Commission (“FTC”), along with five other federal regulatory agencies, have adopted joint rules and guidelines aimed at detecting, preventing and responding to warning signs of identity theft. These rules, also known as the “Red Flag Rules”, go into effect on November 1, 2008.

Under the Red Flag Rules: (i) debit and credit card issuers must develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card; (ii) users of consumer reports must develop policies and procedures to respond to a notice of an address discrepancy received from a consumer reporting agency; and (iii) financial institutions and creditors must develop and implement an identity theft prevention program.

This Alert focuses on the third-listed topic since this topic is most applicable to health care providers. Note that those subject to the Red Flag Rules are required to develop an identity theft program and obtain initial approval of that program by their board of directors (or an appropriate committee thereof) by November 1, 2008. As a practical matter, this means that entities subject to the Red Flag Rules that do not yet have a program in place will generally need to develop a program for approval at their next board or appropriate committee meeting in order to meet the November 1 deadline.

Do The Red Flag Rules Apply To Hospitals And Other Health Care Providers?

The Red Flag Rules require financial institutions and creditors offering or maintaining covered accounts that are subject to enforcement by the FTC under the Fair Credit Reporting Act (“FCRA”) to develop and implement a written identity theft prevention program.

Many in the health care industry have questioned the applicability of the Red Flag Rules to hospitals and other health care providers. Those doing so argue, for example, that health care providers do not act as “creditors” merely by deferring payment for rendered services or that health care providers do not maintain “covered accounts” because their patient accounts are not intended to permit multiple payments.

However, the FTC has, through informal statements, taken the position that hospitals and other health care providers are “creditors” with “covered accounts” to the extent they defer payment for services rendered. The FTC’s position is arguably consistent with language in the Red Flag Rules because, as explained below, hospitals and other health care providers arguably fall within the definition of “creditor”, arguably have “covered accounts”, and likely are subject to FTC enforcement under the FCRA. Because of this, the conservative position is that hospitals and other health care providers are subject to the Red Flag Rules and are required to develop and implement an identity theft program by November 1, 2008.

As explained above, the Red Flag Rules apply to “creditors” that offer or maintain “covered accounts” and that are subject to enforcement by the FTC under the FCRA. Health care providers arguably fall within the definition of a “creditor”. Under the Red Flag Rules, a “creditor” is any person or entity that “regularly extends, renews, or continues credit.” “Credit” is “the right granted by a creditor to a debtor to defer payment of debt or . . . to purchase . . . services and defer payment therefor.” Therefore, to the extent a health care provider defers payment for rendered services, the health care provider would likely be characterized by the FTC as a “creditor”.

Additionally, health care providers arguably offer and/or maintain “covered accounts”. A “covered account” includes (i) an account maintained primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions, or (ii) any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft. A health care provider’s patient accounts would likely be characterized by the FTC as “covered accounts” because they are primarily maintained for personal, family or household purposes and because they involve or are designed to permit multiple payments or transactions by the patient.

Finally, health care providers (both for-profit and not-for-profit) are likely subject to FTC enforcement under the FCRA.

Hence, to the extent a hospital or other health care provider allows a patient to defer payment for medical services rendered by the provider, the FTC would likely consider the hospital or other health care provider as a creditor and require the hospital or other health care provider to comply with the Red Flag Rules.

What Must Hospitals And Other Health Care Providers Do To Comply With The Red Flag Rules?

Entities subject to the Red Flag Rules (“covered entities”) are required to develop and implement a written identity theft prevention program designed to detect, prevent and mitigate identity theft with respect to their covered accounts. Under the Red Flag Rules, covered entities have some flexibility in designing their program since such entities have the opportunity to develop and implement a program that is appropriate to their size and complexity and the nature and scope of their activities and operations. With that said, each identity theft program must include the following basic elements:

- **The program must identify red flags that signal possible identity theft and incorporate the red flags into the program.** “Red Flags” are patterns, practices or specific activities that signal potential identity theft. In identifying red flags, a covered entity should consider the types of covered accounts it offers and maintains, the methods used to open and provide access to such accounts, and any previous experience with identity theft. After identifying the red flags, the identified red flags must be incorporated into the program.

In an appendix to the Red Flag Rules, the FTC and other agencies have identified 26 potential red flags that can be incorporated into a program. Examples of these potential red flags include discrepancies in address and other identifying information (e.g., names, social security numbers, birth dates, etc.); presentation of suspicious documents (e.g., documents that appear altered or forged or a document containing a photograph that does not match the appearance of the customer presenting the identification); unusual use or suspicious activity related to a covered account; and/or notice of unusual activity from customers, victims of identity theft, law enforcement or others. Covered entities should review these and other relevant sources for red flags that might be applicable to their operations and should include these red flags in their identity theft program.

- **The program must detect red flags.** This element requires a covered entity to identify in its policies and procedures actions it can take to check for red flags of identity theft in connection with covered accounts. For example, in the case of opening new accounts, covered entities could require the person opening the account to provide information verifying the identity of the person. Or, in the case of existing covered accounts, covered entities could take measures to authenticate customers, monitor transactions or verify the validity of change of address requests.

- **The program must respond appropriately to detected red flags.** If a red flag is detected by a covered entity, the covered entity must respond to the red flag in a manner that is appropriate to the degree of risk posed. Examples of such appropriate responses include contacting the customer, changing passwords or security codes, reopening a new covered account with a new account number, closing an existing covered account, not opening a covered account or notifying law enforcement.
- **The program must be updated.** Covered entities should update their programs periodically to reflect changes in risks both to customers and to covered entities. A covered entity's update of the program should be based on factors such as the experiences of the covered entity with identity theft, changes in identity theft methods and changes in methods to detect, prevent and mitigate identity theft.
- **The program must have proper oversight.** Covered entities must obtain initial approval of their program from their board of directors (or an appropriate committee thereof). To comply with the Red Flag Rules, this approval should be given by November 1, 2008. Thereafter, the board, a committee thereof, or a designated senior management employee must be involved in the oversight, development, implementation and administration of the program. As part of this oversight, staff responsible for implementing the program should make at least annual reports to the board, a committee thereof or a designated senior management employee regarding the program and its implementation. The covered entity is also required to conduct staff training as necessary to effectively implement the program. Finally, if a covered entity engages a service provider to perform an activity in connection with a covered account, the covered entity must take steps to ensure that the service provider conducts the activity in compliance with policies and procedures designed to detect, prevent and mitigate the risk of identity theft. For example, a covered entity could require the service provider by contract to abide by the covered entity's program or to have in place its own policies and procedures addressing the detection, prevention and mitigation of identity theft.

For more information on developing an identity theft program or if you have questions regarding this Alert, please feel free to contact any of the following, or to the member of the firm who handles your health care matters:

Bryan Looney
bryan.looney@kutakrock.com
(479) 695-1953

Chris Phillips
chris.phillips@kutakrock.com
(402) 231-8787

Mark Sabey
mark.sabey@kutakrock.com
(303) 292-7712

Heather Schmiegelow
heather.schmiegelow@kutakrock.com
(479) 695-1951