Katten

Katten Muchin Rosenman LLP

ClientAdvisory

Mandatory Compliance Date for "Red Flag" Rules Fast Approaching

October 21, 2008

Starting November 1, 2008, all "creditors" must have a board-approved, written Identity Theft Prevention Program ("Program") for their "covered accounts" which is designed to identify, detect, prevent and mitigate against patterns, practices and activities that indicate the possible existence of identity theft.

Why Does it Matter?

On its face, this obligation appears to have minimal significance for health care organizations and providers, as they are not financial institutions or typical commercial creditors, but the Federal Trade Commission ("FTC") has stated that the so-called Red Flag Rules are applicable to health care providers, including both for-profit and nonprofit entities and individual practitioners, if those entities and individuals extend credit (i.e., defer payment) to their patient customers.

Thus, while trade associations such as the American Medical Association have lobbied the FTC to conclude that the Red Flag Rules do not apply to physicians or other health care providers, unless the FTC states otherwise, these groups should take steps to ensure compliance with the Red Flag Rules as of November 1, 2008.

What Are the Origins and Purpose of the Red Flag Rules?

On December 4, 2003, President Bush signed into law the Fair and Accurate Credit Transactions (FACT) Act (Pub. L. No. 108-159). Among other things, the FACT Act added several new provisions to the Fair Credit Reporting Act of 1970 and directed the FTC and several other federal agencies to publish joint regulations regarding the detection, prevention, and mitigation of identity theft. On November 9, 2007, the agencies published such final rules and guidelines. 72 Fed. Reg. 63718 (Nov. 9, 2007).

What Action Must Be Taken?

The Red Flag Rules state generally that a creditor's board-approved Program must be designed to identify, detect and respond to "red flags." The creditor must also periodically update its Program as necessary and appropriate.
To assist with Program development and implementation efforts, the rules include interagency guidelines ("Guidelines") for each of the Program components. Various trade associations, including the American Hospital Association and some of its state chapters, have also developed Red Flag Rules compliance guides and toolkits to assist their members.

- **Identification and Detection of Relevant Red Flags.** The Program must include written policies and procedures to identify and detect red flags. To do so, the Guidelines suggest that creditors consider the types of covered accounts that they open and maintain. Also, what is the method for a client to open and access such an account? What practices or activities might suggest a red flag incident associated with the opening of or request for access to a covered account?

  Recommended Actions:

  1. Health care providers likely maintain multiple types of accounts from which there is a "reasonably foreseeable risk" of identity theft, including patient financial and medical accounts. While the rules may have been motivated by concerns about the financial implications of identity theft, they are equally applicable to medical identity theft concerns and a health care provider's Program should account for such concerns.

2. As with the risk assessment required under the HIPAA Security Rule, health care providers should assess how a would-be identity thief would seek access to a patient/resident's financial and medical accounts and statements. This could include the presentation of suspicious personal identity information, the receipt of questionable change-of-address cards or an urgent request for access to patient files and medical records.
3. A health care provider should take into account prior experiences, if any, with patient/resident identify theft attempts or occurrences when developing its red flag identification and detection policies and procedures.

- **Responding to Red Flags.** In the event that a red flag is detected, the creditor must respond appropriately in order to "prevent and mitigate" identity theft. An appropriate response should account for factors that heighten the risk of identity theft, such as a data security breach with online access to individually identifiable health and personal information. Appropriate responses to red flags may include monitoring of the affected account, contacting the patient/resident, changing passwords/security codes and closing an account.

  Recommended Actions:

  1. Health care providers covered under the HIPAA Privacy and Security Rules should have already developed policies and procedures to respond to "security incidents." However, the Red Flag Rules are separate from the HIPAA Security Rule and it may be best to administer a standalone Program, even if that Program cross-references the provider's HIPAA policies and procedures.
  2. Once a red flag is detected, a health care provider should have established response procedures. Keep in mind that red flags are broadly defined to include patterns, practices and activities that indicate the possible existence of identity theft.
  3. Different red flags may justify different responses. For instance, evidence that a patient's financial account statement was inadvertently included in another patient's envelope will likely justify a different response than evidence indicating that a computer back-up tape of patient financial accounts has been lost.

- **Ensuring That the Program Is Up to Date.** Creditors must periodically review and update their Programs to ensure that those Programs are current and reflect changing risks to the creditor and its customers.

  Recommended Action: Health care providers should pay particular attention to the expanding frequency of medical identity theft. Providers should monitor industry news and, as appropriate, adjust their Program policies and procedures to account for methods employed by medical identity thieves.

- **Board Approval.** All Programs must be approved by the creditor's board of directors or an appropriate committee of the board.

  Recommended Action: Health care providers should obtain board approval of their Programs and such approval should be evidenced by the board minutes and/or a written resolution.

Please contact Brian Annulis at (312) 902-5473 or brian.annulis@kattenlaw.com if you have any questions about the Red Flag Rules or Program requirements.

Katten

Katten Muchin Rosenman LLP www.kattenlaw.com

CHARLOTTE CHICAGO IRVING LONDON LOS ANGELES NEW YORK PALO ALTO WASHINGTON, DC

Katten Muchin Rosenman LLP is an Illinois limited liability partnership including professional corporations that has elected to be governed by the Illinois Uniform Partnership Act (1997). London affiliate: Katten Muchin Rosenman Cornish LLP.

10/21/08