March 2009 www.ssd.com

Deadline Nears for Compliance With Red Flag Rules

In October 2008, Squire Sanders published a Health Care Alert on the fast-approaching deadline for the Identity Theft Red Flag Rules, which were, at time of publication, scheduled for implementation on November 1, 2008. Shortly thereafter, the Federal Trade Commission (FTC) extended the deadline for enforcement of the Rules to May 1, 2009.

The FTC and the federal financial institution regulatory agencies published what have come to be known as the "Red Flag Rules," which require financial institutions and creditors to develop and implement an Identity Theft Prevention Program, 72 Fed. Reg. 63718 (Nov. 9, 2007). Because hospitals and other health care providers typically allow for deferred payment for provided services, most will meet the definition of a "creditor" and therefore must develop and implement such a prevention program. The program must be approved by the organization's governing body, or appropriate committee of the governing body, by May 1, 2009.

The prevention program must include policies and procedures for detecting, preventing and mitigating identity theft, which should be designed to accomplish four goals:

1. **Identify relevant patterns, practices and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those flags into the prevention program.** The Rules define a red flag as a pattern, practice or specific activity that indicates the possible existence of identity theft. Organizations are free to define red flags as they see fit – provided that the types of accounts, the methodology used to open and access the accounts, and the organization's previous experience with identity theft are considered during

Founded in 1890, Squire, Sanders & Dempsey L.L.P. has lawyers in 32 offices and 15 countries around the world. With one of the strongest integrated global platforms and our longstanding one-firm philosophy, Squire Sanders provides seamless legal counsel worldwide.

Contacts:

Scott A. Edelstein
+1.202.626.6602
+1.415.954.0205

John C. Erickson III
+1.614.365.2790

David W. Grauer
+1.614.365.2786

Douglas A. Grimm
+1.202.626.6676

Kristin J. Harlow
+1.614.365.2799

John M. Kirsner
+1.614.365.2722

Kelly A. Leahy
+1.614.365.2839

Robert D. Nauman
+1.614.365.2721

Nicole J. Webb
+1.513.361.1207

Squire Sanders publishes on a number of other topics. To see a list of options and to sign up for a mailing, visit our subscription page.

Cincinnati · Cleveland · Columbus · Houston · Los Angeles · Miami · New York · Palo Alto · Phoenix · San Francisco · Tallahassee · Tampa · Tysons Corner ·

the development of the red flag list.

The Rules provide 26 examples of potential flags that could be incorporated into a prevention program. These include notifications from credit reporting agencies, identification documents or credit applications that appear altered or forged; discrepancies existing between information listed on the credit application and information listed on the credit report; a Social Security Number that has not been issued; or unusual activity on the credit report.

2. **Detect red flags once they have been incorporated into the program.** Once its prevention program is in place, the organization must monitor its effectiveness. For example, when opening a new account, the organization should require sufficient identification to verify the identity of the applicant, and a credit reporting agency should be consulted. A change-of-address request for an existing account should be verified with the patient.

3. **Respond appropriately to any red flags that are detected to prevent and mitigate identity theft.** The response to a red flag should be commensurate to the risk posed by the red flag. Possible responses to red flags include contacting the patient to confirm the status of the account; terminating passwords, account numbers or other access codes and requiring the patient to contact the organization for identity verification; or notifying the authorities.

4. **Ensure the program is updated periodically to reflect changes in the risks from identity theft.** There is no required schedule for updating the prevention program. Rather, the Rules provide that an organization should look to its experience with identity theft, changes in theft methodologies in the marketplace and changes in theft detection methodologies when determining whether, and how, to update the program.

   Annual reports must be made to the board, the appropriate committee or a designated senior management employee. The Rules anticipate staff training as a necessary part of implementation to ensure that, should a red flag arise, the appropriate policies and procedures are followed to detect, prevent and mitigate the potential for identity theft.

   Organizations should also consider amending their business associate agreements with vendors that handle covered accounts, such as billing and collection companies, to ensure their compliance with the new Rules.

Organizations that are not yet in compliance should move quickly to meet the May 1, 2009 deadline. Failure to comply could result in penalties of US$2,500 per violation

under the Fair Credit Reporting Act.

For information on developing an Identity Theft Prevention Program, please contact your principal Squire Sanders lawyer or one of the individuals listed in this Alert.
