FTC RED FLAGS RULE AS IT APPLY TO HEALTH CARE PROVIDERS

Who does the Rule apply to?

The Identity Theft Red Flags Rule[1] was created pursuant to §114 of the Fair and Accurate Credit Transactions Act ("FACTA"). Under these rules, "creditors" and "financial institutions" that have "covered accounts" are required to develop and implement written identity theft prevention programs. The term "creditors" covers all entities that regularly permit deferred payments for goods and services. 16 C.F.R. §681.1(b)(5) For example, creditors include health care providers who render services and bill later, such as hospitals, doctors, and other health care organizations. A "covered account" is an account used primarily for personal, family or household purposes that permits multiple payments or transactions. 16 C.F.R. § 681.1(b)(3). Additionally, a "covered account" is an account for which there is a "reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft…" Id.

These definitions make the Red Flags Rule applicable, in most circumstances, to health care providers. Credit would result, for example, when a provider allows a patient to defer payment for medical services rendered, which is a common practice in the health care industry.

How do we comply with the Rule?

Financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs, "red flags," of identity theft. To aid in this process, the FTC has provided five specific categories of warning signs. The examples provided may or may not be relevant to your practice or organization, but are intended to help you determine what warning signs are relevant to your operations. See 16 C.F.R. Part 681 Appendix A(II).

The five categories of Red Flags include the following:

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
(2) The presentation of suspicious documents;
(3) The presentation of suspicious personal identifying information, such as a suspicious address change;
(4) The unusual use of, or other suspicious activity related to, a covered account; and
(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

After you have identified categories of Red Flags that are applicable to your organization, your program must also address how to detect these Red Flags when opening new covered accounts and maintaining your current covered accounts. See 16 C.F.R. Part 681 Appendix A(III). If you already have programs to monitor patient records and transactions, to identify behavior that indicates the possibility of fraud and identity theft, or to validate patient address

[1] The FTC recently renumbered the Identity Theft Red Flags Rule from § 681.2 to § 681.1.

changes, you should incorporate these tools into your comprehensive identity theft prevention program.

Next, your program's polices and procedures should include appropriate responses to prevent and mitigate identity theft after a Red Flag has been detected. Your response should be proportional to the degree of risk posed by the identified Red Flag. The Guidelines associated with the Red Flags Rule offer the following examples of appropriate responses:

- Monitoring a covered account for evidence of identity theft;
- Contacting the patient or customer;
- Changing passwords, security codes, or other ways to access a covered account;
- Closing an existing account;
- Reopening an account with a new account number;
- Not opening a new account;
- Not trying to collect on an account or not selling an account to a debt collector;
- Notifying law enforcement;
- Determining that no response is warranted under the particular circumstances.

See 16 C.F.R. Part 681 Appendix A (IV). Clearly, some of these responses will not apply directly to your organization, and are merely intended to provide guidance as you identify what responses to include in your program.

Finally, the Rule requires periodic updates to your program to ensure that it keeps current with identity theft risks. As technology changes or as identity thieves change their tactics, it is important to make sure that your program is sufficient to address any new risks to your patient's or organization's personal information. Consider the following factors when updating your program:

- Your organization's experience with identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent, and mitigate identity theft;
- Changes in the types of accounts that your organization offers or maintains; and
- Changes in your business arrangements including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

See 16 C.F.R. Part 681 Appendix A (V).

How do I administer the program?

Your initial written program must be approved by your board of directors or an appropriate committee of your board. If you don't have a board, someone in senior management must approve your program. See 16 C.F.R. Part 681 Appendix A (VI). Your board may oversee, develop, implement, and administer the program or it may designate a senior employee to handle

this. Staff should be trained as necessary to remain up-to-date on the program and how to apply it to your practice or organization's daily operations. Additionally, the person responsible for the program should report at least annually to the board of directors or to a designated senior manager to evaluate the following: (1) how effect the program has been in addressing the risk of identity theft; (2) how you are monitoring the practices of your service providers; (3) significant incidents of identity theft and your response; and (4) recommendations for major changes to the program. Id.

The Red Flags Rule give covered health care providers some flexibility in implementing their identity theft programs, taking into account the size and complexity of a health care provider's business. The Red Flag Rules "underscore … the ability of a … creditor to incorporate into its [identity theft program] its existing processes that control reasonably foreseeable risks to customers or to its own safety and soundness from identity theft." 72 Fed. Reg. 63.740 (November 9, 2007). Accordingly, your Red Flags program may be a part of your HIPAA compliance efforts. Many of the actions needed to comply with the Red Flags Rule already may have been included with your HIPAA compliance policies.

If you have any questions or need further assistance, please feel free to contact either James W. Thomas or Lindsay R. Darling with the Jackson Kelly Health Law Group.