

The Red Flag Rules' Application To The Healthcare Industry

09 October 2008

Article by Alissa D.K. Smith

Identity Theft Programs Must be in Place by November 1, 2008

Identity Theft Red Flag- "a pattern, practice, or a specific activity that indicates the possible existence of identity theft."

On November 9, 2007, the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration jointly issued regulations called the "Red Flag Rules". The purpose of the Red Flag Rules (or, the "Rules") is to combat identity theft. The Red Flag Rules require financial institutions and creditors to implement a program to detect, prevent, and mitigate identity theft in connection with new and existing accounts. For organizations that are subject to the Rules, identity theft programs must be in place by November 1, 2008.

These Rules apply to hospitals, clinics and other healthcare organizations if the organizations meet the Rules' definition of "creditor" and if the organizations offer or maintain "covered accounts". The Red Flag Rules have an unexpectedly broad application because the definition of "creditor" includes any entity that regularly accepts deferred payments for its goods or services. If a hospital, for example, regularly offers payment plans or allows patients to pay in installment payments, the hospital would be considered a "creditor" within the meaning of the Rules. Many in the healthcare industry have been surprised at the broad application of these rules to healthcare organizations because healthcare organizations typically do not think of themselves as "creditors". However, the FTC, in a business alert, specifically stated, "[w]here non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors." This memorandum sets out the tests for determining whether an organization is subject to the Red Flag Rules.

Organizations that are subject to the Rules, must implement board-approved, written, identity theft programs and procedures by November 1, 2008. For healthcare organizations, Red Flag programs will most likely include policies and procedures for detecting, preventing and mitigating medical identity theft that affects accounts such as patient billing accounts and the related medical records. This memorandum summarizes the federal rules and guidelines for structuring identity theft programs.

For healthcare organizations, the FTC is the agency charged with interpreting and enforcing the Red Flag Rules. Failure to comply with the Rules could result in civil monetary fines and enforcement actions.

I. Is Your Organization Subject to the Red Flag Rules?

The Red Flag Rules apply to "creditors" with "covered accounts".

A. Definition of "Creditor"

The Red Flag Rules contain a very broad definition of "creditor". The law defines "creditor" to mean any person who regularly extends, renews, or continues credit. "Credit" means the right granted by a creditor to a debtor to defer payment of debt. An organization is not a "creditor" simply because it accepts credit cards as a form of payment. Rather, the question is whether the organization regularly defers payment for its goods and services. The FTC has not defined the term "regularly". Because there is no clear definition, each organization must determine whether customer payment deferrals occur on a regular basis. Many healthcare providers, such as hospitals and clinics, frequently offer patients deferred payment plans or installment payments, and would, therefore, be defined as a "creditor" under the Red Flag Rules.

B. Definition of "Covered Accounts"

If an organization meets the definition of "creditor", the next step is to determine whether it maintains "covered accounts". A "covered account" is defined as a "continuing relationship" between a person and a creditor in which the creditor maintains or offers the account for the purchase of goods or services for personal, family, household or business purposes, that either: (1) permits multiple payments or transactions (such as credit card accounts, mortgage or car loans, cell phone accounts, or checking or savings accounts); or (2) in which there is a reasonably foreseeable risk to customers or the creditor of identity theft.

Patient billing accounts could fall under the first category of "covered accounts" if organizations permit multiple payments on these accounts. Alternatively, patient billing accounts could fall under the second category of "covered accounts" because of the reasonably foreseeable risk that they would be affected by identity theft. The FTC did not provide examples of the second type of "covered account" because the determination of whether an account falls within the second category will depend on the facts and circumstances related to each type of account that makes it vulnerable to identity theft. **Patient medical records** may fall within the second category of covered accounts because they are particularly vulnerable to medical identity theft, such as in cases when patients change their identity in order to receive narcotics or insurance coverage.

Additionally, the Rules state that in order to meet the definition of "covered accounts", the accounts must be "continuous relationships" with persons, and not simply one-time, limited interactions. It is likely that patient billing accounts and the related medical records would often fall in the category of "continuous relationships" because patients seek medical care on a recurring basis.

II. What are the Components of an Identity Theft "Red Flag" Program?

If an organization meets the definition of "creditor" and maintains "covered accounts", the organization must establish reasonable processes and procedures to combat identity theft in connection with opening and maintaining the covered accounts. For example, a hospital or clinic might establish identity theft Red Flag policies and procedures related to patient billing and medical records, such as a policy which requires patients to present photo identification in order to register or prior to receiving medical care (subject, of course, to EMTALA requirements under which emergency medical care must not be delayed).

The Rules include some basic requirements for establishing and administering Red Flag programs, as follows:

- (1) The program must be in writing;**
- (2) The program must include reasonable policies and procedures to: (i) Identify relevant Red Flags, and incorporate those Red Flags into the program; (ii) Detect Red Flags that have been incorporated into the program; (iii) Respond appropriately to any Red Flags that are detected; and (iv) Ensure the program is updated periodically;**
- (3) The program must be appropriate to the size and complexity of the organization and to the nature and scope of its activities;**
- (4) The organization must consider the FTC's Red Flag interpretive guidelines when establishing its Red Flag program, and include the elements of the FTC's guidelines into the Red Flag program, as appropriate;**
- (5) The program must be formally approved, and regularly reviewed, by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management. Administration of the program must include staff training to effectively implement the program, and must also include oversight of relevant service provider arrangements; and**
- (6) The creditor must periodically conduct risk assessments to determine whether it offers or maintains covered accounts. The risk assessment must take into consideration the methods that the organization provides for opening and accessing its accounts, as well as the organization's previous experiences with identity theft.**

In addition to the basic requirements which are listed above, the FTC published interpretive interagency guidelines to assist organizations in the formation of their Red Flag programs. The FTC does not mandate any specific language, policies or procedures that must be included in an identity theft program. Rather, as long as an organization complies with the basic requirements mandated by the FTC's Rules, each organization has the flexibility to tailor its Red Flag program in accordance with the organization's size and complexity, and the nature and scope of its operations. For some organizations, an identity theft program may be designed as a separate program, with distinct policies and procedures. For other organizations, identity theft programs may be incorporated, as appropriate, into existing policies and procedures and other arrangements. When the FTC is monitoring compliance with the Red Flag Rules, the FTC will be looking for good faith, reasonable efforts to comply with the Rules.

A. Step One: Identifying Relevant Red Flags in Connection with Covered Accounts

An organization's first step is to identify relevant Red Flags. One way to do this is to evaluate points of entry into covered accounts where identity theft may take place, and to determine the Red Flags that the organization should watch for, which may indicate that identity theft has taken place.

The FTC guidelines outline the process that an organization should follow in identifying relevant Red Flags. First, the organization should evaluate the type of covered accounts that the organization maintains. For a hospital or clinic, these will likely include billing and medical records. Second, the organization should evaluate the methods that are available to open the accounts, as well as the possible methods for accessing the accounts. For example, access could occur through patient registration and through updates to a patient's medical record. Finally, the FTC guidelines state that the organization should consider its past experiences with identity theft.

The FTC guidelines lists several identity theft Red Flags that an organization may consider. Those Red Flags include: alerts, notifications or warnings received by consumer reporting agencies or services about fraud detection; the presentation of suspicious documents, such as altered photo identification or insurance cards or a suspicious address change; the unusual use of, or other activities relating to, covered accounts; and notices from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with the organization's covered accounts.

Organizations may find it useful to form an identity theft committee to create identity theft policies and procedures. The committee should consist of personnel from across the organization who are associated with covered accounts. For example, a committee for a hospital may include medical personnel and other staff who are involved with areas in which there is a high risk of identity theft, such as emergency room and pharmacy personnel. The committee should also include staff who are involved with patient entry into the system, such as registration and billing personnel.

B. Step Two: Detecting Red Flags in Connection with Covered Accounts

Next, the organization must identify instances where Red Flags would likely be detected in connection with the opening or accessing of covered accounts. For example, a missing or altered photo ID or insurance card presented at registration could be a Red Flag, and would trigger action, such as refusal to register the patient, in order to control risks of identity theft. Another example of a Red Flag may be an instance or pattern of unusual medical care that appears on a patient's medical chart. In that case, it may be appropriate to contact the patient to confirm with the patient that they are truly the one receiving the care.

C. Step Three: Implementing Prevention and Mitigation Measures; Responding Appropriately to Red Flags

Prevention measures may include, as appropriate, a policy that requires patients to present photo identification upon registration. Further, an organization could require verification of the validity of address changes or authentication measures for insurance coverage, such as placing calls to third party payors. Of course, any detection or prevention measure a healthcare provider adopts must not interfere with the provider's EMTALA obligations to provide immediate screenings and medical care for emergency medical conditions.

The FTC provided guidelines for appropriate responses that an organization may follow if it detects a Red Flag. Appropriate responses may include monitoring the covered account for

evidence of identity theft; contacting the customer to tell them about the suspicious activity; changing password security codes or other devices that permit access to the covered account; reopening a covered account with a new account number; not opening a new covered account if identity theft is suspected; closing an existing covered account; not attempting to collect on the covered account, refunding amounts already collected, or not selling the covered account to a debt collector; or notifying law enforcement or Medicaid Fraud Control Units, as appropriate. In some cases, after monitoring the activity associated with the account, or verifying information, an appropriate response will be no response at all.

D. Step Four: Updating the Red Flag Program

An organization's identity theft program must be updated on a regular basis. The updates should reflect any changes to risks to customers or to the safety of the covered accounts based on instances of identity theft. The FTC guidelines state that updates should also reflect changes in methods of identity theft, changes in any methods the institution has implemented to protect, prevent or mitigate identity theft, changes in the type of accounts that the institution offers or maintains, or changes in any business arrangements the institution has entered into.

III. What About Covered Accounts that are Maintained or Accessed by Service Providers?

The Rules require that organizations exercise appropriate and effective oversight of service provider arrangements. For healthcare entities, an example of a relevant service provider would be a third party billing provider. FTC guidelines state that if an organization engages a service provider to perform an activity in connection with covered accounts, the organization should ensure that the service provider conducts its activities in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. In order to meet the FTC guidelines on working with these service providers, an organization could contractually require the service provider to follow the organization's Red Flag program, or it could require that the service provider establish and follow its own Red Flag program.

IV. How Should Your Organization Administer the Identity Theft "Red Flag" Program?

The Rules require that the program be approved and overseen by the organization's board of directors, an appropriate committee of the board, or a designated employee at the level of senior management. The Rules also require that staff are trained to implement the program, as needed, and that administration of the program. The FTC guidelines state that oversight activities would include: assigning specific responsibilities for the program's implementation; reviewing reports on compliance with the program; and approving material changes to the program.

Additionally, the FTC guidelines recommend that staff responsible for administering the program should report to the oversight body at least annually. The annual report should address the organization's compliance with the program, matters related to the program's effectiveness, material matters related to service provider arrangements, significant instances of identity theft, and any recommendations for changes to the program.

V. Periodic Identification of Covered Accounts

The Rules require that creditors periodically determine whether they offer or maintain covered accounts. As such, creditors must conduct risk assessments to determine whether they offer the accounts, by taking into consideration: (1) The methods the creditor provides to open covered accounts; (2) The methods the creditor provides to access covered accounts; and (3) The creditor's previous experience with identity theft.

VI. Conclusion

The FTC mandates that creditors with covered accounts establish identity theft Red Flag programs designed to detect, prevent and mitigate identity theft in connection with covered accounts. Healthcare organizations should keep in mind that, aside from some basic requirements for Red Flag programs, which are listed above, the FTC allows organizations flexibility in structuring Red Flag programs. Each organization will have different risks related to identity theft. Accordingly, each organization's Red Flag program will be unique, based on the organization's size and complexity, and the scope and nature of its activities. The FTC's Rules and guidelines will help organizations establish reasonable processes and procedures to detect, prevent and mitigate instances of identity theft which could impact their operations, as well as affect the health and safety of patients and customers.

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.