RED FLAG RULES

In November 2007, the Federal Trade Commission (FTC) along with the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, and the Department of Treasury Office of the Comptroller of the Currency and Office of Thrift Supervision jointly issued the *Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003* final rule. To address the risks of identity theft, financial institutions and creditors are required to develop and implement a written identity theft prevention program that detects, prevents, and mitigates identity theft. These requirements are also known as the Red Flag rules and apply to hospitals and other health care providers. Failure to comply with the Red Flag rules can lead to penalties such as civil monetary penalties and regulatory enforcement action.

In addition, the regulations contain requirements for consumer reporting agencies related to the handling of discrepancies between an address contained in a request for a credit report and the address in the consumer reporting agency's file. The third component of the regulations outlines requirements for debit and credit card issuers to implement procedures that assess the validity of address changes under certain circumstances. While these two components are essential to protecting consumers from identity theft, they are not applicable to most health care providers at this time. This brief, therefore, focuses on providing a summary of the Red Flag rules and guidelines and how they affect health care providers.

Legislative History

Identity theft is "a fraud committed or attempted using the identifying information of another person." In 2003, Congress passed the Fair and Accurate Credit Transaction Act of 2003 (FACT Act), extending and updating the Fair Credit Reporting Act to further protect consumers against identity theft. As mandated by section 114 of the law, the FTC and the other regulatory agencies were required to jointly issue regulations requiring financial institutions and creditors to establish reasonable policies and procedures implementing the guidelines regarding identity theft and to identify possible risks to customers or to the "safety and soundness of the institution or customer." The law further required that in developing the guidelines, the regulatory agencies should identify patterns, practices, and specific forms of activities that may alert the financial institution or creditor of the possible existence of identity theft. These agencies must also update the guidelines as necessary. Although a number of agencies are involved in monitoring compliance with the requirements, the FTC is the regulatory authority for health care providers.

Covered Entities

Given the different types of regulatory agencies that were involved in developing the final regulations, it is evident that the provisions of the final rule apply mostly to banks and other financial institutions, such as finance companies and mortgage brokers. The regulations, however, also extend the obligations to *creditors*, a general term that includes health care providers. Consistent with the definition found in 15 U.S.C. 1961a(e) and 1681a(r)(5), a creditor is "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit."

Based on this broad definition, a health care provider may be required to comply with these regulations if they defer payments for goods and services or offer extended payment plans to patients allowing them to make multiple payments. The concern for health care providers is that of medical identity theft for the purpose of obtaining medical services.

Red Flag Regulations and Guidelines

Under the final rule, any organization that maintains or offers covered accounts must develop and implement a written Identity Theft Program that is designed to detect, prevent, and mitigate identity theft. They must comply with this requirement by November 1, 2008. A covered account includes any account that a financial institution or creditor offers or maintains for personal, family, or household purposes that allows for multiple payments or transactions. A covered account also includes any other type of account for which the customer, financial institution, or creditor may be at risk for identity theft, including financial, operational, compliance, reputation, or litigation risk. As a result, prior to developing an identity theft program, as well as periodically thereafter, organizations must determine whether or not they offer or maintain covered accounts. To make this determination, organizations should conduct a risk assessment taking into consideration the following:

1. The methods the organization provides to open accounts;
2. The methods the organization provides to access the accounts; and
3. The organization's previous experiences with identity theft.

This risk assessment process will initially help determine if the organization needs an identity theft program. If based on the risk assessment, the organization concludes that a program is necessary, they can use the results to identify the accounts the program must address. In addition, periodic assessments will help them reassess the accounts for risk of identity theft. On the other hand, if an organization decides that a program is not necessary, periodically conducting this risk assessment allows the organization to reassess the need to develop and implement a program based on changes in the accounts they maintain or other factors.

Guidelines

Given that the regulations apply to a variety of organizations, the regulatory agencies do not provide specific requirements as to the design or content for the identity theft programs. This gives organizations flexibility in tailoring their programs based on their size, complexity, and the nature and scope of their operations. The regulations, however, do offer guidelines that organizations can use to develop and implement their program.

Administratively, to ensure adequate oversight, an organization's Board of Directors or Board committee must be involved in the development, implementation, and administration of the program. They must approve the organization's initial identity theft program as well as any subsequent changes to the program. As part of this oversight, a senior management employee responsible for the implementation and day-to-day administration of the program should provide regular reports to the Board or Board committee. At a minimum, the Board should receive annual reports about the program. These reports should address the effectiveness of the organization's policies and procedures in addressing the risk of identity theft, significant incidents involving identity theft and corresponding response, and recommendations for material changes to the program. In addition, to ensure adequate implementation of the program, organizations should provide training to relevant staff as necessary.

More specifically, the final rule requires that each identity theft program include four basic elements. Each program must include reasonable policies and procedures to:

1. Identify and incorporate relevant Red Flags;
2. Detect Red Flags;
3. Respond appropriately to any detected Red Flags; and
4. Ensure periodic updates to the program.

Identifying and Incorporating Red Flags

The final regulations define Red Flags to be "patterns, practices, or specific activities that indicate the possible existence of identity theft." These Red Flags, singly or in combination, can alert an organization to the possible risk of identity theft to a patient or provider. To identify possible Red Flags, organizations should look into sources of Red Flags, such as any previous incidents of identity theft, methods of identity theft, and applicable supervisory guidance. They should also monitor and stay updated about any changes in the industry regarding identity theft risks. The regulations suggest the following five main categories from which organizations should identify and incorporate Red Flags:

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.

In the final rule, the regulatory agencies provide general examples of Red Flags that organizations can use to incorporate in their identity theft programs. The agencies emphasized that this list is not comprehensive and is just illustrative of the types of Red Flags organizations at a minimum *should consider* incorporating, as appropriate, into their programs. The list of Red Flags provided in the final rule is appended as Appendix A to this brief. Ultimately, the Red Flags an organization chooses to incorporate into the program will depend on the nature and scope of its operations and should be relevant to the risk factors they assessed during the risk assessment of their accounts, such as:

- The types of accounts offered or maintained;
- The methods provided to open the accounts;
- The methods provided to access the accounts; and
- The organization's previous experiences with identity theft.

Detecting Red Flags

As part of their identity theft program, organizations are also required to establish policies and procedures to detect the Red Flags incorporated into the program. These should once again address the risk factors previously mentioned. For example, as it relates to the opening of covered accounts, organizations can detect Red Flags by obtaining information to verify the identity of an individual opening the account. Similarly, as it pertains to accessing existing

accounts, the organization should obtain information to authenticate the person attempting to access the account. Moreover, organizations should establish processes to monitor transactions and verify the validity of change of address requests.

The detection of Red Flags may follow certain precursors that indicate possible risks for identity theft. These include phishing e-mails that persuade individuals to reveal personal identifying information, vishing voicemails that similarly attempt to obtain personal or financial information, and security breaches that involve the theft of personal information.

Responding to Red Flags

To determine whether a detected Red Flag is evidence of the risk of identity theft, organizations must also establish policies and procedures for responding to the Red Flags. These policies should also include a process to conclude that the Red Flag does not indicate a risk of identity theft. The organization's response to the detected Red Flag should correspond to the degree of risk of identity theft posed by the activity. Examples of possible responses to detected Red Flags include:

- Determining the risk of identity theft.
- Monitoring accounts for evidence of identity theft.
- Contacting the patient/customer.
- Changing any passwords, security codes, or other security devices that permit access to a covered account.
- Reopening an account with a new account number.
- Not opening the new account.
- Closing an existing account.
- Notifying law enforcement.

No matter what steps an organization takes to address a detected Red Flag, they should ensure the response is compliant with any applicable legal or regulatory requirements.

Updating the Identity Theft Program

Finally, to ensure organizations maintain effective identity theft programs, the final rule requires the development of policies and procedures to periodically update the program. Organization's should update their programs to reflect the changing risks to patients and "the safety and soundness" of the organization.

Conclusion

In general, although the Red Flag rules may be burdensome for covered entities, they serve an important business and compliance purpose in protecting consumers against the risk of identity theft. The development and implementation of identity theft programs will help organizations detect, prevent, and mitigate incidents of identity theft. With that in mind, the regulatory agencies that jointly issued these final regulations provided these non-prescriptive guidelines to assist organizations adopt an identity theft program that is best suited to their organization.

APPENDIX A

The organization will consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 681.1(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
   a. A recent and significant increase in the volume of inquiries;
   b. An unusual number of recently established credit relationships;
   c. A material change in the use of credit, especially with respect to recently established credit relationships; or
   d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

1. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
   a. The address does not match any address in the consumer report; or
   b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

2. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

3. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
   a. The address on an application is the same as the address provided on a fraudulent application; or
   b. The phone number on an application is the same as the number provided on a fraudulent application.

4. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
   a. The address on an application is fictitious, a mail drop, or a prison; or
   b. The phone number is invalid, or is associated with a pager or answering service.

5. The SSN provided is the same as that submitted by other persons opening an account or other customers.

6. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

7. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

8. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

9. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

<u>Unusual Use of, or Suspicious Activity Related to, the Covered Account</u>

10. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

11. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
   a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
   b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

12. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
    a. Nonpayment when there is no history of late or missed payments;
    b. A material increase in the use of available credit;
    c. A material change in purchasing or spending patterns;
    d. A material change in electronic fund transfer patterns in connection with a deposit account; or
    e. A material change in telephone call patterns in connection with a cellular phone account.

13. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

14. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

15. The financial institution or creditor is notified that the customer is not receiving paper account statements.

16. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

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

17. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.