hen the Red Flags Rule went into effect on January 1, 2011, it brought significant identity theft issues into the spotlight and implications for a wide array of industries. The rule is designed to ensure that organizations have procedures in place to detect and remedy patterns, practices, and activities that indicate the presence of identity theft (“red flags”).

Extremely broad in scope, the rule is enforced by the Federal Trade Commission (FTC), federal bank regulatory agencies, and the National Credit Union Administration. It requires that all organizations subject to the Fair and Accurate Credit Transactions Act of 2003 implement a written identity theft prevention program to detect, prevent, and mitigate identity theft.

With the law now in effect, it is critical for information professionals to determine whether their organizations are subject to the Red Flags Rule, what their organizations must do to comply, and how the rule affects their role as information management professionals.
An information management professional likely will play an important role in the development, implementation, and operation of such a program.

Who Must Comply?
The Red Flags Rule applies to all financial institutions and creditors that offer or maintain covered accounts. (See “Financial Institutions and Creditors” and “Covered Accounts” sections below to learn how these terms are defined.) If the organization falls into one of these categories, it will need to develop and implement an identity theft prevention program that complies with the rule. An information management professional likely will play an important role in the development, implementation, and operation of such a program.

Financial Institutions and Creditors
As defined by the Red Flags Rule, financial institutions include state and national banks, state and federal savings and loan associations, mutual savings banks, state and federal credit unions, and any other entity that holds transaction accounts belonging to consumers. A transaction account is a deposit or other account from which the owner makes payments or transfers, including checking accounts, negotiable order-of-withdrawal accounts, savings deposits subject to automatic transfers, and share-draft accounts.

The Red Flags Rule, as originally drafted, defined a creditor as:
- An entity with covered accounts that regularly extends, renews, or continues credit
- An entity that regularly arranges for the extension, renewal, or continuation of credit
- Any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit

Under this broad definition, a business that sells a product or service on credit should be asking whether it must comply with the rule.

But in December 2010, President Barack Obama signed into law the Red Flag Program Clarification Act of 2010, which significantly narrows the definition of creditor. The earlier broad definition would have required many businesses whose functions were incidental to credit extension, such as medical and legal practices, to take costly measures to prevent identity theft. Because the applicability of the Red Flags Rule to certain organizations was uncertain, and because a number of industry groups (e.g., the American Medical Association and the American Bar Association) raised significant objections, the FTC delayed implementation several times to allow for clarification from Congress.

The act defines creditors as only those entities that “regularly and ordinarily in the course of business”:
1. Obtain or use consumer reports
2. Furnish information to consumer reporting agencies in the course of a credit transaction
3. Advance funds on behalf of a person, based on the obligation to repay

The last category does not include an organization that advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person. The apparent intent of this language is to create an exemption for entities that allow payment to be deferred for a service, unless they engage in one of the three practices listed above.

While the media have reported that lawyers, physicians, dentists, accountants, orthodontists, pharmacists, veterinarians, nurse practitioners, social workers, and other similar service providers are now exempt from the rule, the act did not create any blanket exemptions. Therefore, if a provider “regularly and ordinarily in the course of business” uses consumer reports or reports accounts to consumer reporting agencies, directly or indirectly, that entity may be subject to the application of the Red Flags Rule.

Covered Accounts
If an organization qualifies as a financial institution or creditor under the rule, it must then ask whether it holds covered accounts. There are two types of covered accounts as defined by the rule.

The first type is an account held primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions (e.g., credit cards, mortgage or car loans, cell phone accounts, utility accounts, checking accounts, and most types of savings accounts).

The second type is any account for which there is a reasonably foreseeable risk of identity theft to account holders, or a risk to the safety and soundness of the financial institution or creditor. These might include financial, operational, compliance, reputation, or litigation risks (e.g., small business accounts, sole proprietorship accounts, and single-transaction consumer accounts).

Unlike the first category of consumer accounts designed to permit multiple payments or transactions, which are always covered accounts under the rule, accounts in the second category are covered accounts only if the risk of identity theft is reasonably foreseeable.

An Identity Theft Prevention Program in Action
Any financial institution or creditor that offers or maintains at least one covered account must comply with the Red Flags Rule by developing and implementing a written program designed to detect, prevent, and mitigate identity theft in connection with covered accounts. The program must in-
Warning Signs That Must Be Identified in Identity Theft Prevention Programs

Category 1: Alerts, notifications, or warnings from a consumer reporting agency:
1. Fraud or an active-duty alert on a credit report
2. Notice of a credit freeze in response to a request for a credit report
3. Notice of an address discrepancy provided by a credit reporting agency
4. A credit report indicating a pattern of activity inconsistent with the person’s history (e.g., a big increase in the volume of inquiries or the use of credit, especially on new accounts)
5. An unusual number of recently established credit relationships
6. An account that was closed because of an abuse of account privileges

Category 2: The presentation of suspicious documents:
1. Identification that looks altered or forged
2. Presentation of identification by a person who does not match the photo or physical description on the document
3. A document with information that differs from what the person presenting the document is saying or does not match other information
4. An application that looks altered, forged, or cut up and reassembled

Category 3: The presentation of suspicious personally identifying information:
1. An address that does not match a credit report
2. A Social Security number that is listed on the Social Security Administration Death Master File or that has not been issued according to the Social Security Administration’s monthly issuance tables
3. Information that contains inconsistencies or that has been used on an account known to be fraudulent
4. Incomplete information, such as where a person omits required information on an application and does not respond to notices that the application is incomplete
5. Incorrect or unavailable authenticating information, such as where a person is unable to answer a “challenge question”

Category 4: Unusual use of or suspicious activity on an open account:
1. Requests for new or additional credit cards, cell phones, etc., shortly after a change of address
2. Requests to add new users to an account shortly after a change of address
3. Activity on a new account typically associated with fraud, such as the account holder not making the first payment, making only an initial payment or using most of the available credit for cash advances or for jewelry, electronics, or other merchandise easily convertible to cash
4. Use of an account in ways inconsistent with established patterns, such as nonpayment when there has been no history of missed payments
5. A significant increase in the use of available credit
6. A major change in buying or spending patterns or electronic fund transfers
7. A noticeable change in calling patterns for cell phone accounts
8. Activity on an account that has been inactive for a long time
9. The continuation of account activity when mail sent to the account holder is repeatedly returned as undeliverable
10. Complaints from the account holder that he or she is not receiving statements in the mail
11. Reports of unauthorized charges on the account
12. Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts
... an organization’s information management professionals need to design, implement, and certify the technical integrity of the program.

include reasonable policies and procedures to identify, detect, and respond appropriately to warning signs of identity theft. It must also be updated periodically to reflect the changing risks of identity theft.

There are no specific practices or procedures that must be included in an identity theft prevention program, and the requirements will vary based on an organization’s unique identity theft risk profile. However, the warning signs that must be identified under an identity theft prevention program generally fall into one of the following categories (see sidebar on page 25 for descriptions of each category):

1. Alerts, notifications, or warnings from a consumer reporting agency
2. The presentation of suspicious documents
3. The presentation of suspicious personally identifying information
4. Unusual use of or suspicious activity on an open account

An identity theft prevention program must contain policies and procedures that address detection of these warning signs. For a new covered account, these policies and procedures will likely include obtaining identifying information about and verifying the identity of the person opening the account. For existing accounts, an organization may need to take steps, such as authenticating customers, monitoring transactions, and verifying the validity of change-of-address requests.

An identity theft prevention program must also outline the actions that an organization will take to respond appropriately to detected red flags. Appropriate responses may include:

- Monitoring a covered account for evidence of identity theft
- Contacting the account holder in the manner required by applicable state law
- Having the account holder change his or her password, user name, security code, challenge question, or other identifying information
- Closing the current account and opening a new account with a new account number
- Refusing to collect on a red-flagged account or not selling such an account to debt collectors
- Notifying appropriate law enforcement authorities
- Making a notation on the account that no further response is warranted should the red flags turn out to be innocuous
- Updating the prevention program periodically to reflect the changing risks of identity theft

Role of Information Management Professionals

In today’s technology-driven world, an organization’s information technology systems (or those of third-party service providers) are responsible for processing and storing each customer’s identity, contract, and related personal information. Once an identity theft prevention program is developed and the appropriate physical and administrative security controls are ready to be put in place, an organization’s information management professionals need to design, implement, and certify the technical integrity of the program.

During the process, they may need to consider complex technical issues (e.g., secure user authentication controls, physical and logical access controls), including dynamic passwords; data encryption standards for information transmitted over the Internet or maintained on portable computing devices; monitoring technology for unauthorized use of or access to personal information; and firewall and virus protection for the systems.

According to the Red Flags Rule, the organization’s identity theft prevention program must then be approved by its board of directors or an appropriate board committee. There must also be board-level or senior management oversight of the development, implementation, and administration of the overall program.

Following approval, business and IT staff must be trained to implement, test, operate, and manage the program and related IT systems effectively. The organization must also exercise appropriate oversight of arrangements with third-party service providers that are in a position to identify, detect, and respond to issues related to the Red Flags Rule.

Effectively Mitigating Risks

Without question, the Red Flags Rule affects a wide range of organizations that face a risk of identity theft. In order to comply with the rule, these organizations must define and implement policies and information systems that focus on collecting, analyzing, and managing information about customers and their accounts in order to detect and prevent identity theft.

By understanding the background of the rule and its requirements, information professionals will be in the best position to help their organization develop, implement, and maintain the required identity theft prevention program, as well as the related information systems necessary to meet its legal obligations under the rule. END

James M. Kunick can be contacted at jkunik@muchshelist.com. Neil B. Posner can be contacted at nposner@muchshelist.com. See their bios on page 51.