

## **Warning Flag**

### **Most MSAE Members Are Subject To FTC's New Red Flag Rules. Are You In compliance?**

**By Michael G. Oliva**

Millions of businesses, non-profit organizations, and governmental entities are unaware that the Federal Trade Commission's (FTC) Red Flag Rules ("Rules") for preventing identity theft apply to them. As a result, the FTC has granted a six-month extension for enforcement of the rules.

Any entity that permits deferred payment by individuals or small businesses for goods or services is potentially subject to the Red Flag Rules. Many, if not most, of the businesses and organizations of MSAE members are likely to be subject to the Rules. Every MSAE member's business or organization that has not done so already should conduct a risk assessment immediately to determine if it is subject to the Rules, and an annual assessment thereafter to assure continuing compliance.

Those entities that are subject to the Rules must adopt, implement and administer an Identity Theft Prevention Program before the May 1, 2009 deadline for compliance or risk administrative penalties and potential civil liability.

#### **A Bit of Confusion**

To address the increasing threat of identity theft, the Fair and Accurate Credit Transactions (FACT) Act was enacted in 2003, amending the Federal Fair Credit Reporting Act of 1970. In November 2007, the FTC announced final rules to implement the FACT Act. The so-called "Red Flag Rules" were to take effect November 1, 2008, and applied to "financial institutions" and "creditors" that provide "covered accounts".

Those businesses, non-profit organizations and units of government subject to the Rules were required to have an Identity Theft Prevention Program (ITPP) in place to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

The FTC implemented an outreach program during the past year to explain the Rules. The FTC discovered that millions of businesses and other organizations, which the FTC had intended to be covered by the Rules, were totally unaware that these new rules applied to them. Many paid no attention to the Rules, because they assumed that they were not financial institutions or creditors, since they were not subject to the FTC's other rules governing credit. Many others did not learn that the rules applied to them until it was too late to meet the compliance deadline. In light of these circumstances, the FTC announced on October 22, 2008 that it was delaying enforcement of the Red Flag Rules. The new deadline is May 1, 2009.

## **‘Creditor’ Means Just About Everyone**

The Red Flag Rules apply to financial institutions and other creditors. The definition of a “creditor” is broad enough to include most businesses, non-profit organizations, and even governmental entities. It is likely that the vast majority of the businesses or organizations of MSAE members fall within that definition.

1. **Financial Institutions.** A financial institution means a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other person that, directly or indirectly, holds a transaction account (as defined in section 461 (b) of title 12) belonging to a consumer.
2. **Creditors.** A creditor means 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. *Any business, non-profit, or governmental entity that defers payment for goods or for services is considered to be a creditor under the Rules.*

It should be noted that the Rules do not apply to all transactions by financial institutions and creditors, but only to those that involve “covered accounts.” An account may be a “covered account” under either of two alternative definitions:

1. **Personal Accounts.** An account that is maintained primarily for personal, family, or household purposes that permits multiple payments or transactions. Examples include credit card accounts, mortgage loans, auto loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts.
2. **Other Accounts Involving a Foreseeable Risk of Identity Theft.** Any other kind of account that the financial institution or creditor offers or maintains for which there is a foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks. Specifically, the FTC had in mind that in addition to individual accounts, accounts from small businesses or sole proprietorships were vulnerable to identity theft as well.

Under these definitions, many businesses, non-profits, associations, and governmental agencies are subject to the Rules. Whenever goods or services are provided to and payment is deferred, the provider is a creditor. If the customer is an individual, or if the customer is a small business and there is a foreseeable risk of identity theft, the transaction is a covered account. (Note: Accepting a credit card payment is not considered to be an extension of credit by the seller, but only by the credit card company.)

For example, FTC attorneys have advised hospitals and health care providers that unless they bill and collect for medical services at the same time the services are performed, rather than billing and collecting later, that constitutes a “covered account” and makes the doctor or hospital a creditor subject to the Rules. While the American

Medical Association is protesting that interpretation to the FTC, one can readily see that under the FTC's current interpretation, a very wide range of transactions—and many kinds of businesses, non-profit organizations and governmental agencies who do not normally think of themselves as extending credit—are potentially subject to the Rules.

### **Associations Need Risk Assessment**

The Rules require a risk assessment to determine if a business, non-profit organization, or governmental agency is a financial institution or creditor, and if so, if it provides covered accounts. The FTC estimated that approximately 11 million entities subject to its jurisdiction were likely to fall under the definitions of “financial institution” or “creditor,” and that approximately 2 million of those were likely to have covered accounts requiring adoption of an ITPP.

Nevertheless, all 11 million entities must conduct a risk assessment. Even if the initial risk assessment leads to the conclusion that the Rules do not apply to your organization, a periodic re-assessment is required to assure continued compliance. The assessment should be conducted annually, and the conclusions documented in writing.

### **Create an Identity Theft Program**

Anyone subject to the Rules must develop and implement a written program that is designed to detect, prevent, and mitigate identity theft in connection with opening a covered account, or the use of an existing covered account. The program must consider the FTC's published Guidelines; be appropriate to the size of the organization and the nature and scope of its activities; and may incorporate previously-existing policies and procedures to control identity theft. The program must include reasonable policies and procedures to:

1. **Identify relevant Red Flags for covered accounts, and incorporate them into its program including:**
  - a. Alerts, notifications or warnings from consumer reporting agencies
  - b. Suspicious documents
  - c. Suspicious personal identifying information
  - d. Unusual use of, or suspicious activity relating to, a covered account
  - e. Notice from customers, identity-theft victims, law enforcement, or others regarding potential identity theft
2. **Detect Red Flags that have been incorporated into the program, including:**
  - a. Obtaining identifying information about and verifying the identity of persons opening new accounts
  - b. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests on existing accounts
3. **Respond appropriately to any detected Red Flags to prevent and mitigate identity theft, including:**
  - a. Monitoring accounts for evidence of identity theft

- b. Contacting the customer
  - c. Changing passwords, security codes, and other security devices that provide access to accounts
  - d. Reopening a covered account with a new account number
  - e. Not opening a new covered account
  - f. Not attempting to collect on a covered account or not selling a covered account to a debt collector
  - g. Notifying law enforcement
  - h. Other responses
4. **Update the program periodically to reflect changes in risks from identity theft, including:**
- a. Experiences with identity theft
  - b. Changes in the method of identity theft
  - c. Changes in methods to detect, prevent, and mitigate identity theft
  - d. Changes in the types of accounts offered
  - e. Changes in business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements
5. **Actively implement and administer the program, including:**
- a. Approving a written program by board of directors or an appropriate board committee
  - b. Involving the board, an appropriate board committee, or a designated senior-management level employee in the oversight, implementation, and administration of the program
  - c. Training staff in effective implementation of the program
  - d. Exercising effective and appropriate oversight of service provider arrangements

There are significant administrative penalties, which can be enforced by the FTC and by other federal agencies (and by the various states) for failure to comply with the requirements of the Red Flag Rules. Further, failure to comply and to adopt an effective ITPP may subject a business, non-profit, or governmental entity to lawsuits by victims of identity theft for damages.

Fortunately, there is now time for anyone not previously aware of the Red Flag Rules and the potential applicability of those rules to their own business or organization to conduct a risk assessment, and if necessary, adopt and implement an Identity Theft Prevention Program before the May 1, 2009 deadline.

*Michael G. Oliva (mgoliva@loomislaw.com) is an attorney with Loomis, Ewert, Parsley, Davis & Gotting, P.C. of Lansing, Mich.*

*I:\MGO\MSAE\Red Flag Rules Article from Olivia.doc*