

## **Summary of the FTC Red Flag Rule and Template Policy for use by Covered Associations**

The FTC has announced a delay in implementing new regulations, which would require organizations to implement, so called “Red-Flag” rules. The new regulations will be implemented on June 1, 2010. CAI will continue to monitor and communicate our concerns to the FTC on this issue.

Under the initial proposal, a covered organization to put in place procedures for addressing any ‘red flags’ related to a consumer account when there are indications that the security of a consumer’s identity has been compromised. This document analyzes the pending proposal.

As this rule will impact some CAI members, we are providing this summary information to assist you with understanding its scope and application. CAI’s membership represents a diverse set of individuals and entities, ranging from community association boards, to managers, management companies and community association related business. As such creating compliance information that meets every contingency is not practical. Thus, this information is not legal advice, but rather it is designed to help you work with your counsel to understand the rule’s broad application, to determine the best course of action for your community association or business and to provide you with a sample compliance policy if needed.

### Application to Community Associations

The regulations issued by the FTC provide that any entity that is engaged in providing installment plans where the payment for goods and services is delayed would be required to comply with the requirements of the regulations. While we do not believe that community associations were the target of these provisions, given the broad language and the broad manner in which courts and regulators interpret such language, we believe that the FTC could find that such rules apply to some associations. As such, one response to ensure an association is protected from FTC enforcement would be to put in place a program that complies with the requirements issued by the FTC.

Specifically, the following factors are indications that your community would be required to implement a program to comply with the “Red Flag” rule:

- The association accepts installment payments for assessments, special assessments, capital assessments, reserve assessments or other required payments.
- There is a reasonable risk of identity theft of consumer data, which may be gauged by, but not limited to, such factors as the size of the association, number of employees with access to association member financial records, and frequency of financial transaction with residents.

Again, a reading of the language related to the applicability of this rule and the factors above, it is possible that the FTC would find at least some community associations would fall under the

scope of the regulations. Even so, community associations are likely to be considered at low risk for identity theft and as such, would only be required to adopt a minimal Red Flag policy. Regardless of the legal analysis, adopting a program to address issues of identity theft is the best option to ensure your community meets its obligations to its members. While there are no private rights to sue under the rule and the risk of FTC enforcement might be somewhat low for community associations, adopting a Red Flag policy will ensure compliance as well as implement a best practice for resident financial data.

Based on FTC guidance, CAI has worked to develop a policy template that can be adapted to the needs and practices of specific community associations in consultation with advice of local counsel. That template may be found [here](#). A full analysis of the rule follows.

### Analysis

The Red Flag rule requires that *financial institutions* and *creditors* develop, implement and administer a written identity theft prevention program to identify and flag potential theft of consumer data related to certain covered accounts. For a CAI member, understanding if the rule applies basically requires a determination of whether the association would be considered a “creditor” by the FTC.

First, the rule defines a *financial institution* as 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 entity that holds a “transaction account” belonging to a consumer. Transaction accounts are accounts or deposits from which a consumer can make payments or transfers to third parties. Banks, credit unions and mutual funds with check or debit privileges would fall under this act. Community associations and management companies in most cases would *not* be considered financial institutions under the new rules.

The definition of *creditor*, however, is much broader. Under the rule, creditors include entities that grant loans, extend credit and make credit decisions, as well as businesses, nonprofits or government agencies that allow customers to regularly defer payments for goods and services. While the regulation is not clear as to what frequency of payment deferral is “regular” for purposes of application, where such deferrals provided by associations are more than isolated occurrences, it is likely they would be considered creditors under the rule. Community associations that offer “bill me later” options, installment plans, or similar deferral of payments for assessments or other payments may be covered by the rule. There is a reasonable argument that, as interpreted by case law, an association would not be a “creditor” if a homeowner/member did not have the “right” to defer payments (which many or most likely do not). However, the FTC takes an expansive view of the law’s reach. As such, some members of CAI could be considered creditors under the rule. As the applicability issue is somewhat cloudy and compliance with the rule is not especially difficult, CAI has prepared a sample compliance

policy for associations who wish to comply with the rule or who want to put a policy to provide protections to member financial data.

If an entity is either a financial institution or a creditor, it must also hold a covered account in order to fall under the provisions of the rule. There are two types of covered accounts. The first type of account is a transactional consumer account, such as a credit card, bank account, mortgage or other account, that permits multiple payments or transactions for personal, family or household purposes. The second type of covered account is any account where there is a foreseeable risk to the consumer or to the safety and soundness of the financial institution or creditor from identity theft. These accounts would include both personal accounts and accounts where there is a perceived risk of identity theft. It is likely that if a community association were considered a creditor, it also would be found to have covered accounts under the rule.

### Requirements for Covered Entities

The FTC rule requires a covered organization to establish a program tailored to its size, complexity and the nature of its operations. Such a program must include “reasonable policies and procedures” to achieve the following:

1. Identify relevant “red flags” for new and existing covered accounts
  - That is, identify the red flags of identity theft that are most relevant to the organization’s particular business and incorporate those red flags into the program
2. Detect red flags that have been incorporated into the program
  - Set up procedures to detect those red flags in the organization’s day-to-day business.
3. Prevent and mitigate identity theft
  - Respond appropriately to any red flags that are identified and subsequently detected
4. Update the program
  - Review and update the program periodically (at least annually) to reflect changes in risks to customers or to the safety and soundness of the creditor from identity theft

The rule requires approval of the procedures by the board of directors or an appropriate committee of the board for any entity covered, oversight of service providers who deal with covered accounts, and appropriate training. Annual reports to the board or senior management are also mandated. More information may be found on the [FTC website](#). The final rule may be found in the Federal Register ([16 C.F.R. Part 681](#)). The FTC has also posted a short [web video](#) on compliance issues.