

## FTC Preparing to Enforce Red Flag Rules Beginning August 1, 2009 By Jonathan Bryant, Esq.

On August 1, 2009, the FTC's "Red Flag Rules" regulations regarding identity theft prevention go into effect. In general, the Red Flag Rules require conservancy districts acting as "creditors" to develop and implement written identity theft prevention programs that identify, detect, and respond to patterns, practices, and activities that might indicate that identity theft has occurred (i.e., the "Red flags" signaling identity theft).

The Red Flag rules apply to all "creditors" that offer or maintain one or more "covered accounts." A "creditor" is defined as a person that regularly extends credit, which includes conservancy districts that allow deferred payment of debts. A "covered account" is defined as an account for personal, family, or household purposes that permits multiple payments or transactions and any other account for which there is a reasonably foreseeable risk to the creditor of identity theft. For those conservancy districts that expressly offer financing or deferred payment plans, the rules clearly apply. Even for conservancy districts that do not engage in such practices, though, the rules may yet apply. FTC personnel have indicated that businesses are "creditors" if they do not require full payment up front but rather bill customers after the services are rendered. Thus, barring further guidance from the FTC to the contrary, we advise that conservancy districts consult with their attorneys to determine whether they should comply with the Red Flag Rules.

Thankfully, compliance with the Red Flag rules should not be too burdensome for most conservancy districts. The conservancy district should first identify its covered accounts. For most conservancy districts, covered accounts would be the conservancy districts' customer accounts. Second, the conservancy district should identify potential theft Red Flag events. These may include presentation of photo IDs or other documents that appear to be forged or altered, suspicious changes of address, and customers demanding records containing personal information with unusual urgency or frequency. Third, the conservancy districts should have a mechanism to detect the Red Flags. This should facilitate the conservancy district obtaining identifying information about, and verifying the identity of, new customers. It should also help the conservancy district authenticate customers, monitor transactions, and verify the validity of change of address requests. Complying with this may be as simple as requiring photo IDs for customers (whether new or existing customers) and requiring certain information to verify a customer's identity over the phone, on the web, or by email before any customer-identifying information is disclosed. Fourth, the conservancy district should respond appropriately to any Red Flags that are detected. Appropriate response might include monitoring a customer's account for further evidence of identity theft, contacting the customer, changing passwords or security codes, foregoing collection on a customer account, notifying law enforcement, or taking no further action.

The rules specifically state that a creditor's identity theft prevention program must be "appropriate to the size and complexity" of the creditor and to the "nature and scope of

its activities.” Thus, reasonable common sense safeguards are likely enough for most conservancy districts.

A conservancy district’s board of directors must sign off on the identity theft prevention program, and the conservancy district should train its staff on how to execute the program. Also, where the conservancy district engages third party service providers (e.g., billing agents and management companies), the conservancy district should ensure that such third parties cooperate with the conservancy district to safeguard against identity theft.

*Jonathan Bryant is an associate at Taft Stettinius & Hollister LLP. Reach him at (317) 713-3458 or [jbryant@taftlaw.com](mailto:jbryant@taftlaw.com).*

*These materials have been prepared by Taft Stettinius & Hollister LLP for informational purposes only and are not legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship. No person or organization should act upon this information without first seeking professional counsel.*