McAfee & Taft
A PROFESSIONAL CORPORATION

Is Your Red Flag Program Ready?

McAfee & Taft Email Alert - October 8, 2008

New federal rules require many businesses to adopt a written program to detect and respond to the warning signs, or "Red Flags," that personal identity theft may have occurred. ***Red Flag programs must be in place by November 1, 2008***. Failure to comply can result in a penalty of $2,500 per violation and expose businesses to other potential liability.

The Red Flag rules apply to financial institutions and "creditors," regardless of size, who offer or maintain "covered accounts." A "creditor" is any entity that regularly extends the right to purchase property or services without demanding immediate payment. A business does ***not*** have to charge interest to be a "creditor." The rules apply, for example, to merchants, banks, hospitals, doctors, lawyers, mortgage brokers, automobile dealers, utility companies, and telecommunication companies, among others.

Only creditors with "covered accounts" must adopt a Red Flag program. An "account" is a continuing relationship established to obtain a product or service for personal, family, household, or business purposes. A "covered" account is either a consumer account involving multiple payments, or a business account for which there is a reasonably foreseeable risk to customers or the safety or soundness of the financial institution or creditor.

The rules require a written program, reasonable and appropriate for the business' size and circumstances, that governs how the business will identify, detect, and respond to Red Flags. The program must be adopted by the business' Board of Directors or an appropriate committee, or, if none, by a designated member of senior management. To formulate a Red Flag program, businesses must:

- Assess the different identifying information that the business acquires, the methods by which the information enters the business' system, and how the information is verified and stored;
- Identify the Red Flags particular to its business that can arise;
- Develop procedures for detecting and responding to suspicious circumstances; and
- Effectively communicate the program and implement it in good faith.

Another related new rule requires users of consumer reports, ***including most employers***, to develop policies and procedures for responding to notice of address discrepancies received from consumer reporting agencies. The policies should be designed to enable the user to form a reasonable belief that it knows the identity of the person for whom it obtained the report, and, under certain circumstances, reconcile the address of the person with the consumer reporting agency. The compliance date for this rule also is November 1.

Because the November 1 deadline is quickly approaching, businesses should act now to ensure compliance.

If you have any further questions, please contact your McAfee & Taft attorney or any of the following lawyers:

- **Susan Walker** • 918.574.3014 • susan.walker@mcafeetaft.com
- **Greg Frogge** • 405.552.2383 • greg.frogge@mcafeetaft.com
- **Pat Rogers** • 405.552.2233 • mailto:pat.rogers@mcafeetaft.com
- **Elizabeth Tyrrell** • 405.552.2217 • elizabeth.tyrrell@mcafeetaft.com