

A yellow triangle pointing downwards, located to the left of the 'BLOGS' header.

BLOGS

Update on Red Flags Rule

As we previously discussed in Issue No. 115 of *The GPMemorandum* (January 21, 2009), the new federal “Red Flags Rule” requires certain businesses to establish written programs to detect, identify, and respond to signs of possible identity theft. The rule is aimed at reducing identity theft by making it more difficult for identity thieves to use stolen identity information to purchase goods or services. **Enforcement by the Federal Trade Commission was set to begin August 1, 2009, but has now been delayed (again) until November 1, 2009.** <http://www.ftc.gov/opa/2009/07/redflag.shtm>.

Application of the Red Flags Rule. The Red Flags Rule applies to “creditors” with “covered accounts.” Businesses are considered “creditors” under the rule if they regularly extend credit, for example, by deferring payments owed, by allowing purchases of items on credit, or by arranging or providing financing. Under the rule, however, businesses are required to have a written identity theft program only if they have “covered accounts.” “Covered accounts” include accounts with individuals for personal or household purposes or any accounts that have risk of identity theft. The FTC has issued guidance to franchisors to assist in evaluating whether a franchisor is subject to the Red Flags Rule: <http://www.ftc.gov/bcp/edu/pubs/articles/art14.shtm>.

In some franchise systems, the franchisor may not be subject to the Rule but the franchisees are covered (for example, franchised businesses that provide services on Net 30 payment terms). The FTC recently issued an easy “do-it-yourself” Identity Theft Prevention Program for use by companies that only have a low risk of identity theft, and this online tool may be useful for franchisees that are covered: <http://www.ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm>.

Compliance with the Red Flags Rule. If a business has covered accounts, the Rule requires it to develop a written program to detect, prevent, and mitigate identity theft by noting “Red Flags” indicating possible theft. The warning signs may include forged or altered photo identifications or documents, invalid Social Security numbers, the use of an account that has been inactive for a long period, or signals of possible identity theft discovered during a credit check, such as fraud alerts, address discrepancies, and credit freezes. The Rule is flexible in that the compliance program should be tailored to the nature and risk of the business.