FTC Issues Guidance to Clarify Scope and Requirements of Red Flags for Identity Theft Prevention Rule

June 26, 2013

The FTC has released a guidance document that clarifies the scope of its Red Flags for Identity Theft Prevention Rule ("the Red Flags Rule") and provides a practical four step guide for covered entities to assess compliance.

The Red Flags Rule requires certain businesses and organizations to have in place a written identity theft program designed to detect "red flags" indicative of identity theft and take appropriate steps to prevent it. While the Red Flags Rule has always applied to "financial institutions" and "creditors," the scope of the term "creditors" has generated some confusion. The initial Red Flags Rule defined "creditor" broadly by reference to the definition in the Equal Credit Opportunity Act and arguably covered any company that extended credit by allowing a customer to defer payment. This would include most businesses and service providers, including retailers, doctors, and lawyers.

After allegations that such a broad definition exceeded the FTC's authority under the Fair and Accurate Credit Transactions Act ("the FACT Act"), Congress reacted by passing the Red Flag Program Clarification Act of 2010. The Act clarifies that for the purposes of the FACT Act, creditor means only those creditors that regularly and in the ordinary course of business either: (1) obtain or use consumer reports in connection with a credit transaction, (2) furnish information to consumer reporting agencies in connection with a credit transaction, or (3) advance funds to or on behalf of a person, based on an obligation of the person to repay. The Act further clarifies that creditor does not include an entity that "advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person."

The FTC Guidance expands on the clarification provided by Congress by offering both general guidance and specific "FAQs" concerning the scope of the Red Flags Rule. With regard to the meaning of "regularly and in the ordinary course of business," the Guidance explains that "[i]solated conduct does not trigger application of the rule, but if your business regularly furnishes delinquent account information to a consumer reporting company but no other information, that [would] satisf[y]" the requirement and fall within the scope of the Rule. The Guidance also explicitly advises that a professional who bills clients subsequent to rendering services would not qualify as a creditor under the Rule. On the other hand, the Guidance explains that any business that regularly uses credit reports would be subject to the Rule, even if a third party evaluates the credit reports on the business's behalf.

The Guidance goes on to provide a "four-step process" towards compliance. Specifically, the Guidance advises covered entities to:

• Identify relevant red flags, including alerts from a credit reporting company, suspicious documents,

and personal identifying information suggestive of fraud.
• Detect red flags by considering what procedures would work best in the particular organization.
• Prevent and mitigate identity theft by responding immediately and terminating service as necessary.
• Periodically update the program to stay on top of developments and industry best practices.

While the Guidance provides a helpful resource in facilitating compliance with the Red Flags Rule, companies must undertake their own analyses to customize their identity theft programs to meet the requirements of the Rule.