FTC To Begin Red Flags Rule Enforcement

By Daniel J. Malpezzi

May 20, 2010

On June 1, 2010, the Federal Trade Commission (FTC) will begin enforcing its so-called "Red Flags Rule." The purpose of the Rule is to require development, monitoring and updating of formal board-approved policies and procedures designed to detect, prevent and respond to customer/client data security or other identity theft breaches.The Rule applies to all "financial institutions" and "creditors" maintaining "covered accounts" under the Rule. It was jointly adopted on November 9, 2007 by the FTC, The Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Fed), the Federal Deposit Insurance Corporation (FDIC), the Department of the Treasury Office of Thrift Supervision (OTS) and the National Credit Union Administration (NCUA) under the authority of the Fair and Accurate Credit Transactions Act of 2003 amendments to the Fair Credit Reporting Act of 1970. The OCC, Fed, FDIC, OTS and NCUA have the authority to enforce the Rule as to regulated financial institutions such as banks, savings banks, savings and loan associations and credit unions. The regulation of all other covered entities, including private businesses, falls within the jurisdiction of the FTC.

The FTC has administratively postponed its formal enforcement of the Red Flags Rule four times since its adoption, most recently until June 1, in order to provide sufficient opportunity for businesses and other covered entities to understand the Rule and to develop and adopt compliance programs. The Rule has generated considerable consternation in the business community by virtue of its very broad definitions of "creditor" and "covered account," and will subject many different types of companies to FTC identity theft regulation.

Under the Rule, a "creditor" includes any natural person, governmental body, corporation, partnership, trust, estate or other entity which regularly extends or arranges for credit. This would most obviously include companies that provide or arrange for direct purchase money financing of goods, such as auto dealers, credit card companies, consumer finance companies and retailers. However, the concept of "credit" is defined extremely broadly, and virtually any business which sells a product or provides a service to a customer on an after-the-fact billing basis would be subject to the Rule if it offers a "covered account." This casts a wide net and picks up most commercial and nonprofit organizations, including hospitals, colleges and universities, continuing care retirement communities, nursing homes, assisted living or personal care homes, utilities, cell phone companies, businesses that provide ordinary course or other trade credit and many medical and other professional service providers.

Two categories of "covered account" are included in the Rule. The first is a "consumer account," which is an account that is maintained primarily for personal, family or household purposes and which allows multiple payments or transactions. Such accounts are automatically covered. The second type is any account, including business accounts, maintained by a creditor "for which there is a reasonably foreseeable risk to customers or the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation or litigation risks." This requires a somewhat subjective analysis as to whether maintenance of non-consumer accounts poses any risk requiring compliance with the Rule. Realistically, however, it may be difficult to identify any electronically accessible account that is not potentially vulnerable to a data or information theft attempt through an online "hacking" attack.

Companies that are subject to the Red Flags Rule must develop and implement a written Identity Theft Protection Program

designed to prevent, detect and mitigate identity theft in connection with new and existing accounts. The requirements of the Rule allow for flexibility in crafting a program tailored to the specific risks, facts and circumstances of each covered entity, but there are certain minimum requirements in order for a program to be FTC compliant.

What are the risks of noncompliance with the Red Flags Rule? Under its general enforcement powers, the FTC can levy civil penalties of up to $3,500 per violation, which could be significant if a company has a large number of customer accounts. The FTC can also bring enforcement actions in court to compel compliance, and the civil fines can increase up to $16,000 per violation after a court enters a compliance order. There is no criminal penalty provided under the Rule.

But perhaps the greatest risk in failing to comply with the Red Flags Rule is the threat of liability arising out of potential class actions or other civil cases which might be brought against a business following a data breach incident. While the Red Flags Rule does not specifically provide a right of private enforcement, it is likely that the Rule's standards, guidelines and requirements would serve as the judicial standard of reasonable care in a private civil action asserting losses or damages arising from an identity theft occurrence. A covered business or other organization that has failed to comply with the Rule would almost certainly face a very difficult defense if it found itself as a defendant in such a lawsuit.