

Red Flags Rule Impacts Local Businesses and Professional Practices

By Rebecca Shwayder Aman

On November 1, 2008, the United States Federal Trade Commission (the "FTC") adopted regulations, called the "Red Flags" Rule, which address the detection, prevention and mitigation of identity theft. Identity theft, in general, is any case of actual or attempted fraud using the identification information of another person. The Red Flags Rule requires certain businesses, including many professional practices, and organizations to implement a written Identity Theft Prevention Program to detect the warning signs or "red flags" of identity theft in their day-to-day operations, take steps to prevent the crime and mitigate the damage it inflicts. Enforcement of the Red Flags Rule was initially scheduled to commence on May 1, 2009, but after several extensions, enforcement has been delayed until December 31, 2010. As of that date, if your business or organization is covered by the Red Flags Rule, you must have a written Identity Theft Prevention Program in place and operating.

The determination of whether a business or organization is covered by the Red Flags Rule is not based on its industry or sector, but rather on whether its activities fall under certain definitions. The Red Flags Rule applies to "financial institutions" and "creditors" that maintain "covered accounts." While the definition of a "financial institution" is fairly straight-forward (i.e. banks, credit unions, etc.), the definition of a "creditor" is much broader. This breadth of definition was the source of much litigation and lobbying efforts, as the initial definition of a "creditor" arguably included professionals such as doctors, lawyers and accountants.

Fortunately, on December 7, 2010, Congress passed the Red Flag Program Clarification Act of 2010, exempting many professions from the Red Flags Rule. As of the day of this writing, the bill simply awaits President Obama's signature. In the Red Flag Program Clarification Act of 2010, Congress amended the Fair Credit Reporting Act's definition of "creditor." A "creditor" is now defined as any entity who (a) in the ordinary course of business, obtains or uses consumer reports in connection with a credit transaction; (b) furnishes information to consumer-reporting agencies in connection with a credit transaction, and (c) advances funds "based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of that person." Effectively, the bill was designed to exempt law firms, accountants, doctors, dentists and other service providers from the "Red Flags" rules; it also removes many small businesses from the regulations' reach.

A "covered account" is one that the financial institution or creditor offers primarily for personal, family or household purposes, which involves or is designed to permit multiple payments or transactions, such as credit card accounts, cell phone accounts, checking or savings accounts and some personal or small business accounts. Furthermore, any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft qualifies as a covered account. When considering whether your business or organization maintains any covered accounts, please consider not only whether your

Jones, Blechman, Woltz & Kelly, P.C.

Page 2

customers or other individuals could be harmed by someone fraudulently using their identity but also how your business or organization might be harmed, such as the inability to collect on a repayment obligation.

Failure to implement an Identity Theft Prevention Program may result in civil monetary penalties. Given the potential for penalties, an accurate determination of whether your business or organization qualifies as a “creditor” with “covered accounts” requires a testing of relevant facts. JBWK’s Business Law Group can assist your business or organization with determining whether you are covered and, if so, with preparing and implementing a written Identity Theft Prevention Program to ensure compliance with the Red Flags Rule requirements.