ROBINSON & COLE LLP

ATTORNEY ADVERTISING

AUGUST 2008

Spotlight On: Consumer Financial Services

Red Flags Signal Uncharted Territory for Many Businesses by November 1, 2008

At the end of 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACT Act), an amendment to the Fair Credit Reporting Act (FCRA). The FACT Act requires financial institutions and creditors to create and maintain written programs for identifying "patterns, practices, and specific forms of activity that indicate the possible existence of identity theft."

The definition of "financial institution" under the FACT Act includes not only the traditionally thought of bank, savings and loan association, and credit union, but it also includes any other business that "directly or indirectly holds a transaction account belonging to a consumer." The definition of "creditor" casts an even wider net - it includes *any* business that regularly extends, renews, or continues credit *and* "any assignee of an original creditor who participates in the decision to extend, renew or continue credit." Examples of creditors could include car dealerships, utility companies, mortgage brokers, or the proverbial attempt to catch-all - *any* business that directly or indirectly holds a transaction account belonging to a consumer.

As part of the FACT Act, Congress instructed the Federal Trade Commission and other banking-related agencies to establish guidelines to help businesses develop programs to spot the so-called "red flags" of identity theft. After nearly four years of drafting, re-drafting and public comment, the Comptroller of the Currency, Federal Reserve, FDIC, Office of Thrift Supervision, National Credit Union Administration, and FTC issued their final Red Flag Rules and Guidelines on November 9, 2007. Although mandatory compliance is not required until November 1, 2008, businesses are scrambling to develop or update their programs. Not surprisingly, several companies are touting products that promise compliance.

With new rules come potential new pitfalls, and businesses of all types that maintain consumer credit information are right to be concerned about an uptick in litigation. Vigorous enforcement of the Red Flag Rules should be anticipated by those agencies that draft them. The FTC, for example, expressly has established information security as a priority in its enforcement efforts. Indeed, even without the force and effect yet to come of the Red Flag Rules, the FTC has already brought nearly two dozen complaints against businesses for "security deficiencies in protecting sensitive consumer information." To date, it has done so under its general authority to prevent unfair competition and deceptive acts.

Although written identity theft programs are required only of businesses with "covered accounts," all businesses bear the burden of assessing whether they offer or maintain such accounts. Covered accounts are defined as those primarily for personal, family or household purposes that involve or are designed to permit multiple payments or transactions. Examples listed in the rules include credit cards, mortgages, auto loans, checking and savings accounts, and utility and cell phone accounts. Also considered covered accounts, however, are those accounts for which there is a "reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor."

Notwithstanding their scope, the Red Flag Rules allow businesses to tailor their programs to fit their own size and complexity. In addition, the programs may be established in the form of amendments to a businesses' existing procedures. Regardless of its level of sophistication, however, each program fundamentally must include means of identifying, detecting, and responding to red flags, as well as a system for its own periodic review and improvement. For one thing, the Red Flag Rules require boards of directors-or, at least, appropriate board committees-to sign off on all initial plans. They also recommend policies and procedures for detecting red flags, such as verifying customer identity and monitoring account transactions. Finally, the guidelines describe appropriate responses to red flags, including contacting the

affected customer, changing security codes, and notifying law enforcement personnel.

However helpful, the guidelines are only a start. Undoubtedly, it will be some time before either the agencies or the industry has a solid sense of what constitutes a strong yet workable theft prevention program. In all likelihood, that understanding will be the product of both consensus and contention. Businesses should do their utmost, of course, to foster the former. A good faith effort to comply with the Red Flag Rules is an essential start.

The information in this spotlight should not be considered legal advice. Consult your attorney before acting on anything contained herein.

For more information, please contact Jennifer Rossi at irossi @rc.com or Bradford Babbitt at bbabbitt@rc.com or by calling 800-826-3579.