INTELLECTUAL PROPERTY ARTICLE

ROBINSON BRADSHAW & HINSON

OCTOBER 2008

Recent Federal Actions Tighten Privacy Standards Across the Board

By John M. Conley and Robert M. Bryan

Two recent developments at the federal level are a significant step towards uniform national minimum standards for the protection of personally identifiable information. One development, the implementation of the new "Identity Theft Red Flags" regulations, has been widely discussed. The other, and potentially more significant, development, the FTC's ramped-up privacy standards enforcement program, has barely been mentioned. The identify theft regulations will probably have less impact on business than was originally feared, while the less-discussed FTC activities may bring about important practical changes in companies' duty to protect privacy.

The identity theft regulations represent the most recent step in the evolution of the 1990s-vintage Fair Credit Reporting Act (FCRA), which was amended in 2003 by the Fair and Accurate Credit Transactions Act (FACTA). The identity theft regulations, which FACTA required and which will be enforced by the Federal Trade Commission, were issued in November of 2007 and take effect November 1, 2008. Many businesses have ignored this development since FCRA was historically thought of as applying primarily to credit reporting agencies. But the amendments apply not only to traditional financial institutions and credit reporting agencies but also to a broadly defined category of "creditors." The term "creditor" covers any company that regularly extends, renews, or arranges for credit. The examples given in the regulations include finance companies, automobile dealers, mortgage brokers, utility companies, telecommunication companies, and other companies that allow consumers to pay for purchases over time. Significantly, the term does not appear to cover businesses that merely make credit card sales.

The regulations do not apply to all activities of creditors, but only to "covered accounts." This category has a two-part definition. The first includes any account that the "creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions." The examples given are "a credit card account, mortgage loan, automobile loan, margin account,

cell phone account, utility account, checking account, or savings account." Since the definition requires that the creditor *offer or maintain* the account, simply accepting credit cards should not be covered. Offering a store credit card, by contrast, in all likelihood would be covered. Lending an organization's name to an affinity credit card program is a closer call, but that activity alone probably would not be covered.

The second part of the definition includes any other account that the creditor offers or maintains "for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor" from identity theft. This loosely worded definition apparently focuses more on the nature of the creditor than the details of the account. The official summary gives no specific examples but mentions the government's "belief that other types of accounts, such as small business accounts or sole proprietorship accounts, may be vulnerable to identity theft."

Despite the broad sweep of their coverage, the regulations do not impose a particularly onerous burden. In fact, what they require is probably what any responsible business should be doing anyway. A covered business must -- by November 1, 2008 -- have in place an Identity Theft Prevention Program. The program must include "*reasonable* (our italics) policies and procedures" to detect, prevent, and mitigate identity theft. The key to the program is detecting and responding to "red flags" that signal possible identity theft, including alerts from consumer reporting agencies, the presentation of suspicious personal identifying information, and unusual use patterns in an account.

The recent change in the FTC's approach to privacy in general may be more significant than the FACTA identity theft regulations. Historically, the FTC has focused on making sure that companies lived up to whatever privacy policies they announced. The FTC described its policy as follows: "Using its authority under Section 5 of the FTC Act, which prohibits unfair or deceptive practices, the Commission has brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers' personal information." Companies assumed that the FTC was leaving it up to them to decide what promises they would make -- *if any* -- about privacy and that they could protect themselves by explicitly limiting the representations about security in their privacy policies.

Now, however, the FTC has made it clear that it will also use its Section 5 authority to bring enforcement actions against companies that collect potentially sensitive personal information but do not offer adequate protection, regardless of how much they limit their promises in their privacy policies. Earlier this year, the FTC settled two separate enforcement actions, against discount retailer TJX and data brokers Reed Elsevier and Seisint. The FTC charged "that each engaged in practices that, taken together, failed to provide reasonable and appropriate security for sensitive consumer information." The charges against TJX included storing and transmitting personal information in ways that made it vulnerable to hackers. The FTC charged the data brokers with collecting and storing massive amounts of "sensitive consumer information" -- things like driver's license and Social Security numbers -- and letting customers gain access with easy-to-guess passwords. This laxity resulted in over 300,000 instances of identity theft. All agreed to settlements that will require them to "implement comprehensive information security programs and obtain audits by independent third-party security professionals every other year for 20 years."

Taken together, these two developments reflect a changing privacy security environment with the following new rules:

• The new FACTA regulations extend well beyond traditional financial institutions to a wide range of "creditors" and credit accounts. They do not extend, however, to merchants who do nothing more than accept credit cards.

• Despite their reach, the new regulations do not require especially difficult or expensive preventive actions. In fact, what they require may be nothing more than what the FTC now seems to be demanding of *all* businesses that collect personal data: a reasonable policy to protect customers' privacy and prevent identity theft.

• The enforcement actions to date suggest that the FTC will first use its limited resources to target high-visibility, high-volume offenders. But every company should view the current FTC actions as a warning: any company that collects personally identifiable information is risking legal exposure if it fails to have at least minimally adequate security in place.