INTELLECTUAL PROPERTY ARTICLE

ROBINSON BRADSHAW & HINSON

JUNE 2008

FTC Consent Decree Clarifies Data Security Standards

By John M. Conley and Robert M. Bryan

What type of data security plan is a business legally required to adopt to protect personal information that it collects on its website? While this seems like a basic and straightforward question, the answer has never been clear for businesses operating in the United States. That may be starting to change.

The main reason for the uncertainty has been the lack of a controlling law that directly addresses this question on a nationwide basis. Instead, we are governed by a patchwork of federal and state laws. Federal privacy laws tend to be sector-specific -- for example, HIPAA for health care, Gramm-Leach-Bliley for financial services and the FCRA and FACTA for consumer credit transactions. Different agencies enforce the privacy rules applicable to different sectors, and the definitions of who is covered under these various provisions are still evolving. While many of the general principles carry over from industry to industry, the specific rules vary greatly. In addition, many companies do not operate in any of the covered sectors. On the state side, most states have now followed California's lead in enacting legislation that targets identity theft in several ways (such as notice of data security breaches and protection of social security numbers), but none of these laws impose general requirements of data security. On top of all of this, the major credit card associations are implementing contracts with their participating merchants that require the merchants to be more vigilant and impose liability for security breaches on merchants rather than issuing banks.

While we are still far from having a comprehensive answer to this question for the operators of websites, we now have some guidance on the *minimum required steps* from a surprising source: Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive trade practices. Although the Act was enacted long before anyone worried much about privacy, it may be evolving into the closest thing that we have to a national privacy law. The act is enforced by the FTC itself, not private parties. While the FTC has never imposed particular substantive privacy requirements on companies in the past, it has consistently taken the position that a company that makes representations to the public about its privacy policies must live up to those promises and that the failure to do so may be treated as an unfair or deceptive trade practice.

A new consent decree helps to clarify just what this means and takes the first step towards more generally applicable substantive standards. (A consent decree is a judgment agreed to by the FTC and a company that it is proceeding against.) The defendant was an online retailer called "Life is Good" (www.lifeisgood.com), who conducted a fairly typical online business. In the course of its sales activities, the company collected consumers' names and addresses and the account numbers, expiration dates, and security codes of their credit cards. The challenged privacy policy was also fairly generic, stating that "We are committed to maintaining our customers' privacy. We collect and store information you share with us . . . All information is kept in a secure file and is used to tailor our communications with you." According to the FTC, Life is Good violated this promise in several ways, including by storing credit card information in clear, readable text; by retaining credit card security codes; by failing to assess its vulnerability to foreseeable hacker attacks; and by failing to use available security and monitoring techniques.

The consent decree requires Life is Good to implement a "comprehensive information-security program." The program must include the designation of employees to coordinate security protection; the identification of internal and external security risks; the creation and implementation of appropriate safeguards against those risks; the monitoring of the safeguards' effectiveness; the oversight of service providers that have access to personal information from Life is Good's customers; and the evaluation of the program's overall efficacy.

On a practical level, it seems fair to assume that the FTC believes that all of these elements are necessary to fulfill a general commitment to "maintaining our customers' privacy" and keeping their personal information "in a secure file." Thus, any company that has any kind of privacy policy should probably be doing all of these things. The FTC has made available a useful guide that describes an acceptable security program in more detail at http://www.ftc.gov/infosecurity/. While this booklet does not technically have the force of law, it does seem to reflect the FTC's thinking about how its general rules should be applied, and it provides a workable outline for any company interested in adopting a reasonably priced data security program.

The FTC action does not relieve any business from the obligation to comply with more extensive industry-specific or state requirements. Nevertheless, it is a useful first step in bringing some level of certainty and consistency to this area.

Robinson, Bradshaw & Hinson, P.A. is a corporate and commercial law firm with more than 125 attorneys. The firm has offices in Charlotte and Chapel Hill, North Carolina, and Rock Hill, South Carolina. For over forty years, the firm has consistently provided innovative solutions to its clients' business needs from both a legal and practical perspective. The firm serves as counsel to public and closely held corporations operating in domestic and foreign markets; limited liability companies; limited and general partnerships; individuals; municipal, county and state agencies; public utilities; health care institutions; financial institutions and tax-exempt organizations. For more information on Robinson, Bradshaw & Hinson, please visit our Web site at www.rbh.com.