SEPTEMBER 2010

PRIVACY LAW ALERT

from the Privacy & Information Security Group of Poyner Spruill LLP

"Reasonable" Security: The FTC Requires It, But What Is "Reasonable" Security?

by Kate Paradise

The Federal Trade Commission (FTC) has taken more than 25 actions alleging that inadequate information security constituted an unfair trade practice in violation of the FTC Act. In these enforcement actions, the FTC has targeted corporations for failure to implement "reasonable and appropriate security measures" and requires in the subsequent consent orders that the organizations implement a comprehensive written information security program and submit to third-party assessments of that program every other year for the duration of the order (usually 20 years).

But what does "reasonable security" really mean? And more important, how do you apply reasonable security measures to your business? Although you can rely to some extent on technology standards and industry best practices, information security law has evolved to a point where case law and FTC enforcement actions are a source of some suggestions.

A recent action against Twitter illustrates that having a defensible password security policy is a crucial security element. The FTC faulted Twitter for permitting "weak" administrative passwords – consisting of only common dictionary words written using all lowercase letters, and containing no numbers or symbols. In addition, Twitter's system failed to lock out users after multiple unsuccessful login attempts. Lack of reasonable safeguards allowed an automated password-guessing program to gain access to the Twitter system after thousands of login attempts. In a separate breach, a hacker who compromised a Twitter employee's personal e-mail account was able to guess a Twitter administrative password because two similar passwords were stored in plain text within that employee's e-mail. The FTC cited storage of passwords in an e-mail account among the "unreasonable" practices Twitter employed.

In another enforcement action, the FTC pursued restaurant chain Dave & Buster's for failure to provide reasonable and appropriate security for credit and debit card data stored on its networks. Credit card information that was collected at in-store terminals, transferred to in-store servers, and finally transmitted to a third-party credit card processing company was intercepted by hackers because the company failed to detect and prevent unauthorized access to the computer networks. The FTC faulted Dave & Buster's for failing to conduct security investigations, failing to monitor system logs, and for not using readily available security measures to limit access to its computer networks through wireless access points. The FTC specifically noted the lack of data loss prevention software and an intrusion detection system when alleging the unreasonableness of Dave & Buster's information security program.

These and other FTC cases provide insight into the policies and practices that are necessary to support a "reasonable and appropriate" information security program. Demonstrating that you have implemented such a program is crucial to mitigate the risk of an unfair trade practices charge by the FTC. Our Privacy and Information Security Practice can help you evaluate your information security program to ensure that it addresses your compliance and risk objectives, as well as areas highlighted by past FTC and other government agency enforcement actions.

Kate Paradise may be reached at 919.783.2886 or kparadise@poynerspruill.com.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW