

New FTC Standards for Data Security?

By **Kenneth K. Dort**

When the Federal Trade Commission, in conjunction with the White House, promulgated its [Consumer Privacy Bill of Rights](#) in February 2012, one of the more intriguing considerations was that the FTC appeared to be setting up a matrix by which a company's voluntary decision to adopt that matrix could become the basis for an FTC enforcement action. Now, after several months, it should be back at the forefront of data security considerations for U.S. businesses.

Earlier this summer, the FTC used that matrix in authorizing a federal action against Wyndham Worldwide Corp. and three of its subsidiaries – a development that highlights a possible change in stance from FTC Commissioner J. Thomas Rosch and illustrates for businesses the importance of developing detailed data/privacy policies.

In its action, the FTC's asserted claim is based entirely upon the alleged violation of the Wyndham group's own internally generated and approved privacy/security policy. In particular, the FTC [complaint alleges](#) that the hotel group's "privacy policy misrepresented the security measures that the company and its subsidiaries took to protect consumers' personal information." The agency charges that the hotel's security practices as represented to the public were "unfair and deceptive" and thus violated the FTC Act.

Rosch voted with a unanimous majority of FTC Commissioners to authorize the federal action against Wyndham, but had dissented from the same portion of the FTC's privacy report and recommendation, which accompanied the release of the Consumer Privacy Bill of Rights in February.

This apparent development at the FTC will bear continued observation across the United States business community, and, at the same time, presents an excellent opportunity for all companies handling sensitive data to conduct an immediate evaluation of their privacy/data security policies and practices to assure that their practices are in complete alignment with their policies. Specific issues of concern include:

- > Enforcement and litigation risks and developments;
- > Contingency breach response planning (including breach notification efforts to affected persons and relevant governmental agencies);

- > Incident response planning (including possible external forensic investigations and law enforcement involvement); and
- > Global/cross-border notification obligations.

In this case, the key to the FTC's charges appears to be that one security breach allegedly facilitated other later breaches. In particular, the FTC alleges that the hotel group first learned in September 2008 of a data breach to its system through one of its properties (which first occurred in April 2008). According to the FTC's allegations, the security flaws exploited in that initial breach were not corrected, and, thus, allowed two subsequent breaches in March 2009 and late 2009.

Approximately 120,000 consumer payment card records were accessed in those two later breaches, according to the FTC's allegations, and were used by various crime syndicates to make fraudulent purchases totaling approximately \$10.6 million. These compromised records were in addition to the 500,000 consumer payment card records compromised in the first breach, according to the FTC.

This enforcement action highlights the importance of developing clear and detailed data/privacy policies that:

- > Implement "best practices" for protecting private consumer data;
- > Maintain compliance with those practices; and
- > Regularly update those practices to track ongoing technical advances.

Significantly, consumers are submitting their confidential data to companies in reliance on those companies' stated practices and policies. The FTC is apparently now going to hold those companies to their public pronouncements in this sphere. Perhaps more importantly, it also demonstrates that, despite some early public misgivings from at least one Commissioner, the FTC now seems intent upon using this enforcement power in the federal courts to force compliance with these companies' previously stated privacy policies.

For additional information, please contact:

Kenneth K. Dort | (312) 569-1458 | Kenneth.Dort@dbr.com

Mary Devlin Capizzi | (202) 230-5101 | Mary.DevlinCapizzi@dbr.com