Cybersecurity Special Report: Trade Commission Takes Hard Line on Data Security

JUDGE AGREES THAT ABSENCE OF ADEQUATE SAFEGUARDS CAN REPRESENT AN UNFAIR TRADE PRACTICE.

Karin McGinnis & Todd Taylor

National Law Journal
11.2014

MVA Privacy & Data Security team co-leaders Karin McGinnis and Todd Taylor were published in *National Law Journal*'s Cybersecurity Special Report on November 24. Their article, "Trade Commission Takes Hard Line on Data Security," discusses *FTC v. Wyndham Worldwide*, in which it was ruled that the Federal Trade Commission could pursue a claim that a company's failure to have adequate data security measures is an unfair trade practice.

The article can be seen below in its entirety. *Reprinted with permission from* National Law Journal*. Copyright 2014 ALM Media Properties LLC. Further duplication without permission is prohibited. All rights reserved.*

Trade Commission Takes Hard Line on Data Security

Judge agrees that absence of adequate safeguards can represent an unfair trade practice.

On April 7, Judge Esther Salas in Newark, in FTC v. Wyndham Worldwide, ruled that the Federal Trade Commission could pursue a claim that a company's failure to have adequate data security measures is an unfair trade practice. In its recent brief on appeal, the FTC made clear that it is not backing down. The agency believes that data security is a basic responsibility of any company that accepts consumer personal information, and that savvy companies should heed Wyndham's lessons.

In the United States, there is no single privacy and data security law of general applicability. There are, however, many federal and state laws that impose obligations on a wide number of different actors.

For example, federal governmental entities are subject to information-security and privacy requirements under laws including the Federal Information Security Management Act and the Privacy Act; financial institutions are subject to privacy and data security rules under the Gramm-Leach-Bliley Act; and certain covered institutions in the health care industry (and their service providers) are subject to rules regarding the use, disclosure and protection of health care-related information under the Health Insurance Portability and Accountability Act and certain related laws and regulations. At the state level, 47 states have enacted data breach notification laws involving personally identifiable information.

Perhaps one of the most wide-reaching and flexible laws in the privacy and data security arena does not even mention the words "privacy" or "data." Section 5 of the Federal Trade Commission Act, a product of the Progressive era, provides that "unfair or deceptive acts or practices in or affecting commerce … are … declared unlawful." The statute defines unfair practices to include those that "cause or [are] likely to cause substantial injury to consumers [and are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." The FTC is granted power to enforce these prohibitions. At its core, Section 5 is a consumer protection statute, and the FTC has interpreted its enforcement writ to cover the regulation of consumer privacy and data security.

The FTC has frequently used its enforcement authority to pursue companies for what it asserted were deceptive acts—issuing privacy policies to consumers that promised more than the companies delivered. The FTC has also interpreted its authority to ensure that companies maintain adequate consumer data security. An example can be found in an FTC enforcement action brought against Tower Records. According to the FTC's complaint, Tower operated a website that allowed users to purchase music and other products. To make purchases, consumers would input personal information, including their names, billing addresses and other contact information. Tower's privacy policy promised consumers that it used state-of-the-art technology to protect the information and that no one other than the consumer could access the data. In the process of a website redesign, however, Tower apparently failed to fully update software code—an "easy" fix, according to the FTC—and, as a result, customer data were viewable by unauthorized visitors to the Tower site.

The FTC argued that Tower Records' failure "to detect and prevent vulnerabilities in their Web site and applications," along with the misstatements in its privacy policy, violated Section 5. As is generally the case with FTC enforcement actions, Tower ultimately entered into a consent order with the FTC rather than challenge the FTC in court.

THE WYNDHAM CASE

That brings us to Wyndham. Wyndham Worldwide Corp. operates and manages hotels, resorts and timeshares through subsidiaries and franchisees. Between 2008 and 2010, Wyndham's computer networks were allegedly breached on three occasions, which led to the loss of more than 600,000 payment-card account numbers and millions of dollars in fraudulent charges.

The FTC brought an enforcement action against Wyndham (and various related parties) asserting that "failure to maintain reasonable and appropriate data security for consumers' sensitive personal information" violated both the deception and unfairness prongs of Section 5(a).

Unlike many targets of FTC enforcement actions, Wyndham decided to contest the FTC allegations, moving in federal court to dismiss the complaint. Wyndham argued that the agency must formally promulgate data security regulations, to provide adequate notice to parties before asserting unfairness claims based on data security incidents.

Salas rejected Wyndham's arguments. Of particular interest, the court found that the language in Section 5, the FTC's guidance on reasonable data security measures and prior FTC consent agreements and opinions give companies adequate notice of appropriate data security standards. Although the court cautioned that "this decision does not give the FTC a blank check to sustain a lawsuit against every business that has been

hacked," the case made clear that the FTC can and will pursue companies for inadequate data security.

Wyndham appealed to the U.S. Court of Appeals for the Third Circuit. On Nov. 5, the FTC submitted a brief to the court in which it made clear that companies are responsible for keeping data "turned over" to them by consumers "from falling into the wrong hands." Although the FTC claims that Section 5 does not require "perfect security," it does require "reasonable" measures. The agency claims it has warned companies for almost a decade as to what measures are reasonable.

What steps should companies take (and what recommendations should their legal, compliance and information-technology advisers provide) in light of the Wyndham decision? A good starting place is to follow the implicit logic of the opinion and look at past complaints and consent orders in which the FTC alleged Section 5 violations due to poor security practices. By avoiding some of the failures cited, a well-advised company might find itself better insulated against FTC enforcement actions.

Below are just a few examples of security failures that the FTC has alleged constitute unfair or deceptive trade practices:

- Failing to restrict employee access to data on a need-to-know basis.
- Failing to adequately train employees to securely dispose of personally identifiable information.
- Failing to use readily available security measures to limit wireless access to retail company networks, thereby allowing intruders to connect wirelessly to in-store networks without authorization.
- Failing to require network administrators and other users to use strong passwords or different passwords to access different programs, computers and networks.
- Failing to encrypt sensitive personally identifiable information.
- Failing to employ sufficient security measures for detecting and preventing unauthorized access to corporate networks on which sensitive data were processed.
- Overriding default secure-socket layer protocol settings in application program interfaces to be used with apps running on mobile and tablet devices, thus leading to the risk of man-in-the-middle attacks.
- Failing to contractually require vendors to implement appropriate security measures to protect personally identifiable information (such as through use of encryption).

In addition, companies should become familiar with the FTC's publication, Protecting Personal Information Guide for Business, which provides practical advice. For technical guidance in implementing or refining data security programs, look to security standards promulgated by well-regarded organizations including the ISO/IEC 27001/2 standards, NIST Special Publication 800-53, the NIST Cybersecurity Framework and the Payment Card Industry Data Security Standard.

Although the FTC has a long history of pursuing Section 5 enforcement actions against companies with lax data security processes, the Wyndham case establishes a judicial precedent that the FTC has authority to safeguard consumers against poor data security. Companies are now on clear notice that they must take reasonable security measures to protect sensitive consumer data in their possession.

However, there is a large body of FTC enforcement actions, decisions and guidance, as well as several well-regarded security standards put forth by an assortment of industry groups, that provide a working framework for legal, compliance and I.T. professionals as they develop or enhance the security programs of their companies and clients.