KING & SPALDING

Client Alert

Privacy & Information Security Practice Group

November 25, 2013

Attacked On All Fronts

FTC Defends Its Authority to Sue Companies That Are Victims of Hacking for "Unfair" Security Practices

Getting hacked by Russian hackers three times in two years has turned out to be only half of the problem for Wyndham Worldwide Corporation. The Federal Trade Commission, in a broad interpretation of the authority granted to it by Congress, brought suit against the hotel franchiser on August 9, 2012. The FTC alleges that Wyndham deceived consumers because its website privacy notice contained misrepresentations regarding Wyndham's privacy practices. The FTC also alleges that Wyndham engaged in "unfair business practices" because it did not have adequate security measures in place to protect customers from unnecessary and unjustifiable risk.

The FTC's allegation that Wyndham engaged in "unfair business practices" has sparked controversy. While most practitioners do not contest that the FTC has authority to bring an enforcement action against a company for misleading or false statements regarding its security practices, a heated debate is ongoing over whether the FTC has the authority to regulate the way companies keep and protect personal data. In its motion to dismiss, Wyndham argued, among other things, that the FTC cannot regulate corporate security practices because it has not published rules governing cybersecurity standards that would provide adequate notice to companies of the standards to which they are being held.

The FTC maintains that unreasonably poor security practices constitute "unfair" acts or practices because it causes or is likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.[1] Just what constitutes a "reasonable," and thus "fair," security system, however, has not been made clear by the FTC in any official rule or policy making process. The FTC alleges that Wyndham's security measures fell short of "reasonable" because Wyndham failed to use complex user IDs and passwords, firewalls and network segmentation between the hotels and the corporate network. In addition, the FTC alleges that Wyndham allowed improper software configurations which resulted in the storage of sensitive payment card information in clear readable text.

Judge Esther Salas of the United States District Court for the District of New Jersey held a hearing on Wyndham's motion to dismiss on November 7, 2013. At the close of the hearing, Judge Salas stated that she hoped to

For more information, contact:

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Sarah E. Statz
+1 404 572 2813
sstatz@kslaw.com

Andrew M. Mutter
+1 404 572 4705
amutter@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street N.E.
Atlanta, GA 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com

issue an order "rather quickly." When Judge Salas issues her order, it will be the first time a court has weighed in on whether the FTC has broad authority to regulate the consumer data security practices of all companies.

Since 2002, the FTC has increasingly asserted its authority to bring injunction actions against businesses that fail to adequately protect consumer data, regardless of whether those companies engage in the activities that bring them under the explicit jurisdiction of the FTC through such statutes as the Gramm-Leach-Bliley Act. The FTC has primarily brought lawsuits against companies after they have been hacked or their security system has otherwise been breached. Indeed, 15 of the 18 formal complaints that the FTC has filed against companies in the past 3 years have all come after a serious incident of deliberate hacking or inadvertent breach of a company's data system was made public.[2] Of those 18 lawsuits, all but the pending Wyndham case has resulted in a consent decree with the FTC.[3] Consent decrees often come not only with steep monetary penalties, but with regular monitoring by the FTC.

Recommendations

Cybersecurity is an area of increased focus for the FTC and the FTC's message is clear: reactive compliance with breach notification requirements is insufficient; companies are required to accurately describe their privacy practices to consumers and implement proactive security measures to protect consumer data. While the FTC has not provided clear guidance on how to proactively protect consumer data and legislation has been deadlocked in Congress for years, clients can take steps to minimize the risk that the FTC will deem their security practices inadequate.

Clients should review their website and mobile application privacy notices frequently to ensure that the notice fully and accurately describes the organization's privacy practices. The FTC is increasingly concerned over any use of data that would "surprise" a consumer, focusing often on mobile application privacy practices. In addition, clients should implement comprehensive privacy and data security policies and assess their security measures to ensure that they are adequately protecting sensitive data. The FTC's reasonableness standard is not concrete, but security measures should be commensurate with the volume and sensitivity of the data being processed and stored. Strong passwords, network segmentation, firewalls, and encryption of sensitive personal information are key steps to ensuring your security measures are "reasonable" in the FTC's eyes.

King & Spalding's Privacy and Information Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Privacy & Information Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 30 Privacy & Information Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy.

* * *

[1] Response in Opposition to Defendant's Motion to Dismiss, Civ. Act. No. 2:13-cv-01887-ES-JAD, Doc. No. 110, pp. 1-2 (May 20, 2013).
[2] *See generally*, Legal Resources: Data Security, Case Highlights, BUSINESS.FTC.GOV (available at **http://business.ftc.gov/legal-resources/29/35**) (last accessed November 15, 2013).
[3] *Id.*