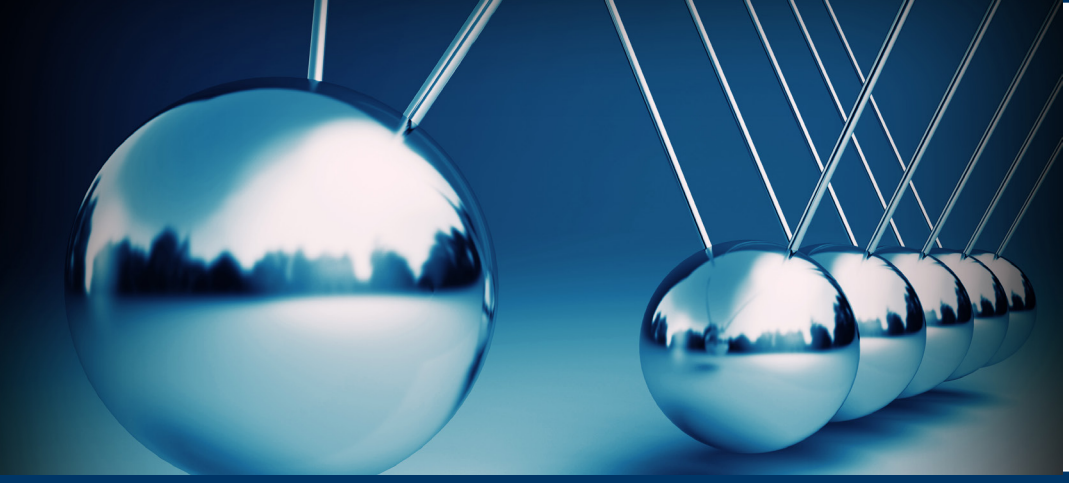

MURTHA MEANS
MORE
INDUSTRY INSIGHT

INFORMATION SECURITY AND PRIVACY GROUP NEWS

THE INCREASED RISKS OF NOT PROTECTING CUSTOMER INFORMATION IN DATA BREACHES

***FTC v. Wyndham Worldwide Corp.* and the Risk of Claims for Unfair or Deceptive Cybersecurity Policies and Practices**

Companies that fail to protect personal information collected in the course of their business operations risk enforcement actions by the Federal Trade Commission (FTC) as well as potential civil penalties, restitution orders and injunctive relief under the Federal Trade Commission Act (the Act). The Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[1] A recent decision from the Third Circuit Court of Appeals in *FTC v. Wyndham Worldwide Corp.*,[2] highlights the types of conduct which would support a claim that a company's cybersecurity policies or practices are "unfair" or "deceptive" to customers and potentially lead to liability.

The Court began its decision by noting that the FTC has been bringing administrative actions under the Act[3] against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers since 2005, and that most of the cases have resulted in settlement. So, the FTC's prosecution of such claims is not new. Nor is the fact that these cases, like many governmental actions, resolve in settlements. This case seems to have resolved, at least for now, any question that the FTC has authority to bring such actions under the "unfairness prong" of the Act.

FTC SUES HOTEL OWNER FOR OVERSTATING ITS DATA SECURITY

The FTC sued hotel owner and operator Wyndham Worldwide, along with several subsidiaries, in June 2012, alleging that "[o]n three occasions in 2008 and 2009 hackers successfully accessed Wyndham Worldwide Corporation's computer systems. In total, they stole personal and financial information for hundreds of thousands of consumers leading to over $10.6 million dollars in fraudulent charges." In the first of two counts, the FTC alleged that Wyndham acted "deceptively" in representing through the privacy policy on the company's website that it "had implemented reasonable and appropriate measures to protect personal information against unauthorized access." The privacy policy stated, in part: "We safeguard our Customers' personally identifiable information by using industry standard practices." The "standard practices" identified within the policy included encryption of data "to protect confidential information . . .

[1] 15 U.S.C. § 45(a).
[2] 799 F.3d 236 (3d Cir. N.J. 2015)
[3] Specifically, § 45(a)

If you have any questions about any matters involving Information Security and Privacy issues, please feel free to contact:

Heather O. Berchem
hberchem@murthalaw.com

Burt Cohen, Chair
bcohen@murthalaw.com

Michael P. Connolly
mconnolly@murthalaw.com

Jennifer A. Corvo
jcorvo@murthalaw.com

Rachel Snow Kindseth
rkindseth@murthalaw.com

James F. Radke
jradke@murthalaw.com

Stephanie Sprague Sobkowiak
ssobkowiak@murthalaw.com

David R. Sullivan
drsullivan@murthalaw.com

Suzanne Brown Walsh
swalsh@murthalaw.com

Edward B. Whittemore
ewhittemore@murthalaw.com

from loss, misuse, interception and hacking." The practices also included the maintenance of fire walls "to ensure that [customer] Information is used only as authorized . . . and that the Information is not improperly altered or destroyed." The FTC alleged that this policy was deceptive because it overstated Wyndham's actual efforts at cybersecurity since, as the FTC alleged, the company did not in fact use encryption, fire walls or other commercially reasonable means of protecting customer information.

FTC's CLAIMS OF INADEQUATE DATA SECURITY PRACTICES

In its second count, the FTC alleged that Wyndham acted "unfairly" under the Act through its failure "to employ reasonable and appropriate measures to protect personal information against unauthorized access." Specifically, the FTC alleged that Wyndham employed inadequate data security practices, including the following:

a. failing to use readily available security measures, such as firewalls, to limit access between the company's hotel property management systems and the Internet;
b. allowing software at the hotels to be configured inappropriately, resulting in the storage of payment card information in easily readable text;
c. failing to remedy known security vulnerabilities on servers;
d. allowing certain servers to connect to the company's network, even though the server manufacturer's default user IDs and passwords were enabled on the servers, and those default IDs were publicly available to hackers through Internet searches;
e. failing to employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess;
f. failing to employ reasonable measures to detect and prevent unauthorized access to the company's computer network or to conduct security investigations;
g. failing to follow proper incident response procedures, including failing to monitor the company's computer network for malware used in a previous intrusion; and
h. failing to adequately restrict third-party vendors' access to the hotels' network, such as by restricting connections to specified IP addresses or granting temporary, limited access, as necessary.

Wyndham argued that none of these alleged failures were "unfair" as that term is used in the Act and, therefore, Wyndham could not be liable under the Act. The Court of Appeals disagreed, based on the legislative history of the Act and the plain meaning of the term "unfair." In doing so, the Court concluded that the FTC has authority to regulate cybersecurity under the unfairness prong of the Act.

It is important to note that, in its decision, the Court of Appeals did not make any findings that any of the above alleged failures actually occurred, nor did it conclude that Wyndham was liable for any of these alleged failures. Those issues remain to be decided as the case moves forward at the trial court level.

THREE IMPORTANT STEPS TO TAKE TO REDUCE THE RISK OF DATA SECURITY CLAIMS BY THE FTC UNDER THE ACT

The *Wyndham* decision serves as a caution to companies that collect personal information from consumers and raises at least the following three important points:

First, a company should be extremely careful about what its privacy policies say about the steps the company is taking to protect personal information. The policies should, of course, be truthful, but should also be as clear as possible and should only commit the company to take steps that it understands (e.g., what is an "industry standard practice?") and is willing and able to carry out.

Second, once a policy is in place, a company should, at a minimum, ensure that its cybersecurity practices match what the published policy says. For example, if a policy says a company uses firewalls or encryption, the company actually should be using firewalls or encryption. Relatedly, when a company says it uses "industry standard practices," it then needs to implement such practices and continuously monitor changes to the industry standards. Due to the ever-changing nature of threats to companies' computer systems, implementation of a company's data security program is not a one-time event.

Third, once a data breach occurs, and in addition to the disruption, expense, and reputational damage that a data breach can cause, there is also a risk that the FTC or similar state regulators will begin enforcement actions to seek remedies on behalf of the injured consumers. While attacks on computer systems may be inevitable and unstoppable in today's world, having a clear privacy policy that is implemented and updated in good faith will go some way to avoiding a claim by a regulator, such as the FTC, that a company has acted "unfairly" or "deceptively" toward its customers.

If you have any questions regarding this issue, please contact:

Michael Connolly (Boston, MA) at 617.457.4078 or mconnolly@murthalaw.com or

Burt Cohen (New Haven, CT) at 203.772.7714 or bcohen@murthalaw.com.