MURTHA MEANS
MORE
INDUSTRY INSIGHT

INFORMATION SECURITY AND PRIVACY GROUP NEWS

December 2015

CRITICAL CYBERSECURITY POLICIES AND PRACTICES AFTER THE SETTLEMENT ORDER IN FTC v. WYNDHAM WORLDWIDE CORP.

Companies are threatened daily by attacks that expose customer credit card and other information stored on company servers, personal computers and other devices. It is, therefore, critical that companies do these three things:

1. Develop and implement a comprehensive written information security program;
2. Routinely assess the effectiveness of that program; and
3. Maintain adequate records to demonstrate the efforts taken to safeguard customer data.

If there is a breach and a loss of customer data, a company faces claims not only by customers, but by regulators such as the Federal Trade Commission ("FTC"). A recent settlement agreement in a lawsuit the FTC filed against hotel owner and operator Wyndham Worldwide Corp. and several of its subsidiaries ("Wyndham") illustrates the ongoing need to establish, monitor, and update data security programs as part of the ordinary course of business. Failure to do so may result in a court order that ultimately requires the implementation of such a program, but that also requires time-consuming, burdensome, and costly compliance with ongoing regulatory oversight.

The FTC's lawsuit following Wyndham's data breach

The FTC sued Wyndham in June 2012, claiming 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 [credit card] charges." On December 11, 2015, after more than three years of litigation, the court entered a Stipulated Order for Injunction ("Order") which contained the terms of a settlement agreement between the parties. Even though Wyndham did not admit that it had violated the law as the FTC alleged, the company nonetheless agreed to a detailed and wide-ranging program of remedial efforts in order to resolve the FTC's claims.

If you have any questions about the issues addressed here, or any other matters involving Information Security 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

Wyndham's agreement to the terms of a comprehensive data security program plus long-term FTC monitoring in order to resolve the FTC's lawsuit

Under the Order, among other things, Wyndham is obligated to:

- Establish and implement a comprehensive written information security program that is designed to protect the security, confidentiality, and integrity of credit card data that it collects. This program must be maintained for 20 years.
- Designate one or more employees to coordinate and be accountable for the company's information security program.
- Develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding credit card data.
- Identify material internal and external risks to the security, confidentiality, and integrity of credit card data that the company collects.
- Evaluate and adjust the information security program based on the results of testing and monitoring or any other changes in circumstances.
- Annually obtain and provide to the FTC a written assessment of the company's compliance with an "Approved Standard," which was identified in the Order as PCI DSS (Payment Card Industry Data Security Standard) or any other standard approved by the FTC.
- Design and implement reasonable safeguards to control the risks identified through the risk assessment and regularly test the effectiveness of the safeguards.
- For a period of 10 years, provide a copy of the Order to all controlling principals and board of director members and to all company officers and employees having responsibility for implementing the terms of the Order.
- Submit a compliance report, certified as truthful by a senior corporate officer, within 1 year of the Order that describes in detail whether and how the company is in compliance with the Order.
- Keep for 3 years after the date of each assessment report all materials relied upon to prepare the assessment.
- Allow the FTC to monitor Wyndham's compliance with the Order through discovery requests and other means under the FTC Act for 23 years from the date of the Order.

It remains to be seen whether the FTC will seek orders requiring similar protective and remedial measures in all future cases involving claims of data breaches. However, many of the terms of the Order mirror the best practices that industry experts recommend in order to attempt to mitigate the risk of loss in the first place.

It is not possible to prevent hackers altogether from attempting to breach a company's data networks. But it certainly would be prudent for a company to take many of the steps set forth in the Order in the *FTC v. Wyndham* case in order to show that it has developed and maintained a program that is reasonably designed to protect its customers' data. Doing so will likely put a company in a better position both to protect its data and, if necessary, to argue in response to a later action by regulators that an assessment of penalties or imposition of other remedial relief, including any ongoing regulatory monitoring of a company's systems, are unnecessary and unwarranted.

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.