Is the FTC Coming After Your Company Next?

Court Affirms FTC Authority in Cyber Security

Online Tech – Webinar
April 29 2014

Tatiana Melnik
Melnik Legal PLLC
tatiana@melniklegal.com | 734-358-4201

Outline

- Why are we here?
- Where are we going?
- Questions?

Why are we here?

- ***Federal Trade Commission v. Wyndham Worldwide Corporation, et al.***
  - Opinion published on April 7, 2014
  - U.S. District Court – New Jersey
  - First court to evaluate authority of the FTC to take action against companies for poor cybersecurity practices

Who is the FTC?

- Federal Agency
- Mission
  - Protect consumers and promote competition
  - Nation's leading privacy enforcement agency
  - Turns 100 years old this year

FTC Authority

- Gramm-Leach-Bliley Act (GLBA)
  - FTC Safeguards Rule
    - implements GLBA
    - provides data security requirements for non-bank financial institutions
- Fair Credit Reporting Act (FCRA)
  - "requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information, and imposes safe disposal obligations on entities that maintain consumer report information"
- Children's Online Privacy Protection Act (COPPA)
  - "requires reasonable security for children's Information collected online"

Testimony of Edith Ramirez Chairwoman of the FTC before the Senate Committee on Homeland Security and Governmental Affairs April 2 2014

FTC Authority – Section 5

- Section 5 of the FTC Act –
  - Prohibits "unfair or deceptive acts or practices in or affecting commerce." (15 USC 45)
  - The prohibition applies to **all persons and companies** engaged in interstate commerce.

FTC Authority – Section 5

- Section 5 of the FTC Act –
  - Prohibits "unfair or deceptive acts or practices in or affecting commerce." (15 USC

"A company acts deceptively if it makes materially misleading statements or omissions."

FTC Authority – Section 5

- Section 5 of the FTC Act –
  - Prohibits "unfair or deceptive acts or practices in or affecting commerce." (15 USC

"A company engages in unfair acts or practices if [1] its data security practices cause or are likely to cause substantial injury to consumers that is
[ ] neither reasonably avoidable by consumers nor
[ii] outweighed by countervailing benefits to consumers or to competition."

Does a Breach = Enforcement?

- No – as the FTC recently testified before the Senate:

> Through these settlements, the Commission has made clear that:
> [1] reasonable and appropriate security is ***a continuous process*** of assessing and addressing risks;
> [2] that there is no one-size-fits-all data security program;
> [3] that the Commission does not require perfect security; and
> [4] that ***the mere fact that a breach occurred does not mean that a company has violated the law***.

The *Wyndham* Case

- Wyndham Worldwide Corporation and several subsidiaries ("Wyndham")
  - Hospitality industry
  - Operates a number of well-known brands
  - Allegation:

    Defendants' ***failure to maintain reasonable security*** allowed intruders to obtain unauthorized access to the computer networks of Wyndham Hotels and Resorts, LLC, and several hotels franchised and managed by Defendants on ***three separate occasions in less than two years***

    Complaint at ¶ 2

The *Wyndham* Case

- The FTC further alleged that Wyndham's security failures led to

  (1) fraudulent charges on consumers' accounts,

  (2) more than $10.6 million in fraud loss, and the

  (3) export of hundreds of thousands of consumers' payment card account information to a domain registered in Russia.

  In all three security breaches, **hackers accessed sensitive consumer data by compromising Defendants' Phoenix, Arizona data center**.

  Complaint at ¶ 2

The *Wyndham* Case

- Property Management System
  - Reservations
  - Check-in/Check-out
  - Credit card payments
- Linked to corporate network, which includes a central reservation system
  - System managed by Wyndham, *not* by owners of Wyndham-branded hotels
  - Wyndham set the rules of the road and collected fees to manage the network

The *Wyndham* Case

- Deceptive statements
  - "Since at least 2008, Defendants have disseminated, or **caused to be disseminated, privacy policies or statements on their website** to their customers and potential customers."

The *Wyndham* Case

- Deceptive statements

"... We recognize the importance of protecting the privacy of individual-specific (personally identifiable) information collected about guests, callers to our central reservation centers, visitors to our Web sites, and members participating in our Loyalty Programs (collectively 'Customers') ...."

The *Wyndham* Case

- Dec

"... We rec
privacy of
informatio
central res
and memb
(collective

"We safeguard our Customers' personally identifiable information **by using industry standard practices**. Although "guaranteed security" does not exist either on or off the Internet, **we make commercially reasonable efforts** to make our collec ion of such Information consistent with all applicable laws and regula ions.

The *Wyndham* Case

- D

Currently, our Web sites **utilize a variety of different security measures** designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company, including the use of 128-bit encryption based on a Class 3 Digital Certificate issued by Veri sign Inc. This allows for utilization of Secure Sockets Layer, which is a method for encrypting data. This protects confidential information - such as credit card numbers, online forms, and financial data - from loss, misuse, interception and hacking. We **take commercially reasonable efforts** to create and maintain "fire walls" and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent with this Policy, and that the Information is not improperly altered or destroyed.

The *Wyndham* Case

- What does it mean to use "commercially reasonable efforts" when considering data privacy and security and cyberliability?
- Tough question to answer.
- What did Wyndham NOT do?

The *Wyndham* Case

a. Firewalls – "failed to use readily available security measures to limit access between and among the Wyndham-branded hotels' property management systems, the Hotels and Resorts' corporate network, and the Internet, such as by employing firewalls;"
b. Encryption – "allowed software at the Wyndham-branded hotels to be configured inappropriately, resulting in the storage of payment card information in clear readable text;"
c. Policies/Procedures of partners – "failed to ensure the Wyndham-branded hotels implemented adequate information security policies and procedures prior to connecting their local computer networks to Hotels and Resorts' computer network"

The *Wyndham* Case

d. Fix known problems – "failed to remedy known security vulnerabilities on Wyndham branded hotels' servers that were connected to Hotels and Resorts' computer network, thereby putting personal information held by Defendants and the other Wyndham branded hotels at risk. For example, Defendants permitted Wyndham-branded hotels to connect insecure servers to the Hotels and Resorts' network, including *servers using outdated operating systems* that could not receive security updates or patches to address known security vulnerabilities;"

The *Wyndham* Case

e. Used default passwords - "allowed servers to connect to Hotels and Resorts' network, despite the fact that well-known default user IDs and passwords were enabled on the servers, which were easily available to hackers through simple Internet searches;"
f. No password rules - "failed to employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess. Defendants did not require the use of complex passwords for access to the Wyndham-branded hotels' property management systems and allowed the use of easily guessed passwords."

The *Wyndham* Case

g. No inventory – "failed to adequately inventory computers connected to the . . . network so that Defendants could appropriately manage the devices on its network;"

h. No intrusion detection – "failed to employ reasonable measures to detect and prevent unauthorized access to Defendants' computer network or to conduct security investigations;"

i. No intrusion response – "failed to follow proper incident response procedures, including failing to monitor Hotels and Resorts' computer network for malware used in a previous intrusion; and"

j. No controlled access – "failed to adequately restrict third-party vendors' access to [the] network and the Wyndham-branded hotels' property management systems, such as by restricting connections to specified IP addresses or granting temporary, limited access, as necessary."

The *Wyndham* Case

- Suffered three separate data breaches
- Attack no. 1 - April 2008
  - brute force attack
  - caused multiple-user lockouts

"Defendants did not have an adequate inventory of the Wyndham-branded hotels' computers connected to its network, and, therefore, although they were able to determine that the account lockouts were coming from two computers on Hotels and Resorts' network, they were unable to physically locate those computers. As a result, Defendants did not determine that the Hotels and Resorts' network had been compromised until almost four months later."

The *Wyndham* Case

- Attack no. 2 - March 2009
  - Access gained into the network through a service provider's administrator account in the Phoenix data center.
  - After customers complained, searched network and found the same malware that was used in attack no. 1
- Attack no. 3 - "Late 2009"
  - Learned of the attack from a credit card issuer

The *Wyndham* Case

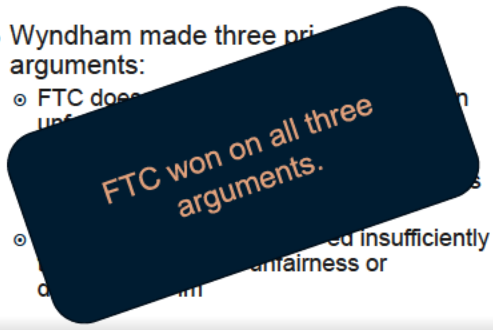
- June 26, 2012 – FTC filed suit in Federal Court in Arizona
- March 25, 2013 – Motion granted to move suit to Federal Court in New Jersey
- April 7, 2014 – Judge issued decision denying Wyndham's motion to dismiss

The *Wyndham* Case

- Wyndham made three primary arguments:
  - FTC does not have authority to assert an unfairness claim in the data-security context
  - FTC must formally promulgate regulations before bringing its unfairness claim
  - FTC's allegations are pleaded insufficiently to support either an unfairness or deception claim

The *Wyndham* Case

- Wyndham made three pri… arguments:
  - FTC does… …n
  - …ed insufficiently
  - …unfairness or



The *Wyndham* Case

- Why is Wyndham fighting so hard?
  - Argues
    - should not be responsible for any lapses in security at its business partners
    - its Privacy Policy clearly only applied to Wyndham and not to its Franchisees
  - 20 year compliance period

Where are we going?

- Expect enforcement actions to continue
- Time to review your existing practices
  - Are they "commercially reasonable"?
  - What are your requirements of vendors?
- What do your contracts say?
  - When was the last time your privacy policy was reviewed?
  - What do your indemnification provisions say? Are there caps on damages?

Where are we going?

- Other FTC settlements to review
  - *In the Matter of HTC America, Inc.* (2013) - http://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter
  - *In the Matter of GMR Transcription Services, Inc.* (2014) - http://www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter
- On-going case
  - *In the Matter of LabMD, Inc.*
    - Administrative case - http://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter
    - Federal case - *LabMD Inc. v. FTC*, No. 1:14-cv-00810, U.S. District Court for the Northern District of Georgia

Disclaimer

This slide presentation is informational only and was prepared to provide a brief overview of hot topics in healthcare. It does not constitute legal or professional advice.

You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Melnik Legal PLLC would be pleased to assist you on these matters.

Any Questions?

Tatiana Melnik
734.358.4201
tatiana@melniklegal.com