What We Know

ARTICLES & INSIGHTS

ABOUT THE AUTHOR

Caren Enloe leads Smith Debnam' s consumer financial services litigation and compliance group. In her practice, she defends consumer financial service providers and members of the collection industry in state and federal court, as well as in regulatory matters involving a variety of consumer protection laws. Caren also advises fintech companies, law firms, and collection agencies regarding an array of consumer finance issues. An active writer and speaker, Caren currently serves as chair of the Debt Collection Practices and Bankruptcy subcommittee for the American Bar Association's Consumer Financial Services Committee. She is also a member of the Defense Bar for the National Creditors Bar Association, the North Carolina State Chair for ACA International's Member Attorney Program and a member of the Bank Counsel Committee of the North Carolina Bankers Association. Most recently, she was elected to the Governing Committee for the Conference on Consumer Finance Law. In 2018, Caren was named one of the "20 Most Powerful Women in Collections" by *Collection Advisor*, a national trade publication. Caren oversees a blog titled: Consumer Financial Services Litigation and Compliance dedicated to consumer financial services and has

Lessons to be Learned from Wyndham Hotels Data Breach

February 2, 2016 | by

The FTC recently entered into a Consent Order last week with Wyndham Hotels and Resorts resolving the FTC's allegations that Wyndham did not do enough to prevent its customer's credit card data from three data breaches that occurred in 2008 and 2009. The Consent Order comes on the heels of the Third Circuit's opinion in the case in which the court held that the FTC has an authority to hold companies accountable for failing to safeguard consumer data. *See Federal Trade Commission v. Wyndham Worldwide Corp.,* 799 F. 3d 236 (3rd Cir. 2015).

Specifically, the Complaint alleges that:

- Wyndham allowed its hotels to store payment card information in clear, readable text;
- Wyndham allowed the use of easily guessed passwords to access the property management systems;
- Wyndham failed to use readily available security measures such as firewalls to limit access between the hotels' property management systems, corporate network, and the Internet;
- Wyndham did not ensure that its hotels implemented adequate information security policies and procedures;
- Wyndham failed to restrict access of its network and servers from third party vendors;
- Wyndham failed to employ reasonable measures to detect and prevent unauthorized access to its computer network or to conduct security investigations;
- Wyndham did not follow proper incident response procedures. Wyndham did not monitor its network for malware used in the prior intrusions. As a result, the hackers in each of the three breaches used similar methods to gain access to credit card information.

Specifically, the FTC's complaint alleges that on three separate occasions in 2008 and 2009 hackers gained access to Wyndham's network and property management systems and obtained unencrypted information on over 619,000 consumers. The complaint alleges that Wyndham participated in deceptive and unfair acts or practices related to

been published in a number of publications including the Journal of Taxation and Regulation of Financial Institutions, California State Bar Business Law News, Banking and Financial Services Policy Report and Carolina Banker.

their data security by failing to address the weaknesses of its cyber security systems that had led to prior attacks.

The Consent Order, which will remain in effect for twenty years, requires Wyndham, among other things:

- To establish and implement a comprehensive written information security program that is reasonably designed to protect the security, confidentiality, and integrity of its customer's credit card data;
- To annually obtain written assessments of its compliance with certain agreed upon data security standards; and
- To maintain records of its efforts, including audits, policies, and assessments which may be accessed by the FTC upon request.

Businesses which store private personal information should take note of the FTC Consent Order and take the following lessons to heart:

- Develop a Written Information Security Program ("WISP") which identifies reasonably foreseeable internal and external risks to the security and confidentiality of customer information that could lead to the unauthorized disclosures of private personal information;
- Continually assess the sufficiency of the institution's safeguards and operational risks including detecting, preventing and responding to attacks against the institution's systems;
- Evaluate and adjust the WISP in light of relevant circumstances and changes in the company's environment, business offerings and operations, as well as the results of security testing and monitoring;
- The FTC has established through the Wyndham litigation that it has authority to bring claims against businesses for cybersecurity intrusions under Section 5 of the FTC Act's unfair and deceptive umbrella;
- The FTC expects all businesses to adhere to the cybersecurity practices required by Section 5 of the FTC Act; and
- Businesses should carefully monitor FTC Consent Orders regarding data breaches and use those consent orders to better model their practices.

CONTACT US

919.250.2000
mail@smithdebnamlaw.com

RALEIGH OFFICE

The Landmark Center
4601 Six Forks Road, Suite 400
Raleigh, NC 27609

Phone: 919.250.2000
Fax: 919.250.2100

CHARLESTON OFFICE

171 Church Street
Suite 120C
Charleston, SC 29401

Phone: 843.714.2530
Fax: 843.714.2541