What We Know

ARTICLES & INSIGHTS

FTC Agrees to Settle with Hardware and Software Provider over Data Privacy Breaches

May 12, 2016 | by

A recent settlement by the FTC with the manufacturer of computer routers serves as a reminder to all that in the growing ***Internet of Things,*** it is critical for companies to have effective security measures in place to protect consumer's private data. The FTC's latest proposed consent order targets Taiwan-based computer hardware maker ASUSTek Computer, Inc. ("ASUS"). ASUS manufactures and sells home routers and related software and services for consumer use. ASUS's routers include software features that allow consumers to access and share files via a wireless connection through their routers. The FTC complaint contends that ASUS routers are prone to multiple vulnerabilities and that critical security flaws within the router's software "put the home networks of hundreds of thousands of consumers at risk." *FTC Press Release: ASUS Settles FTC Charges that Insecure Home Routers and "Cloud" Services Put Consumers' Privacy at Risk* (Feb. 23, 2016).

With no admission of liability, the parties have agreed to a consent order which requires ASUS to adopt a comprehensive security program subject to independent audits for the next twenty years. Here are the key takeaways:

- ***Take Reasonable Steps to Secure Software Features from Vulnerabilities.*** According to the complaint and proposed consent order, ASUS did not take reasonable steps to secure its routers and software add-ons. The FTC showed particular concern that the products at issue were routers which the FTC noted: "typically function as a hardware firewall for the local network, and act as the first line of defense in protecting consumer devices on the local network." The ASUS routers at issue were setup with the same default username and password, and their add-on software's web applications included multiple vulnerabilities that could allow unauthorized access via the router's IP address – information the FTC contends is easily discoverable.

- ***Put Processes in Place to Promptly Address Security Vulnerabilities.*** According to the complaint and proposed consent order, ASUS did not address security flaws in a timely manner and did not notify consumers of the risks. The FTC alleges that

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 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.

updated firmware was provided initially only to affected routers and was not made available to all registered users until several months later.

The Consent Order should be reviewed by all companies involved in the Internet of Things as a risk management tool.

It requires:

ASUS to fully and accurately make disclosures to consumers regarding the extent to which the company or its products or services maintain:

- The security of any covered device;
- The security, privacy, confidentiality or integrity of any covered information;
- The extent to which a consumer can use a covered device to secure a network; and
- The extent to which a device is using up-to-date software.

ASUS to develop and maintain a comprehensive written security program ("WISP") reasonably designed to address security risks related to the development and management of their devices and to protect the privacy, security, confidentiality and integrity of consumer information. The WISP should, among other things:

- Identify internal and external risks to privacy, security, confidentiality and integrity of consumer personal information; and the identification of risks should take into consideration all relevant operations, including product design, development, research, and secure software design development.
- Identify internal and external risks to security of their devices what could result in unauthorized access and the identification of risks should take into consideration all relevant operations, including product design, development, research and secure software design development;
- Assess the company's processes in reviewing, assessing and responding to both third-party security vulnerability reports and to attacks, intrusions or system failures;
- Design and implement safeguards from the outset to identify potential security failures and verify that access to devices and consumer information is restricted consistent with a user's security settings;
- Regularly test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;
- Continue to evaluate and adjust the WISP as needed in light of the results of testing and monitoring.

CONTACT US

919.250.2000
mail@smithdebnamlaw.com

RALEIGH OFFICE

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

CHARLESTON OFFICE

171 Church Street
Suite 120C
Charleston, SC 29401

Phone: 919.250.2000
Fax: 919.250.2100

Phone: 843.714.2530
Fax: 843.714.2541