September 6, 2017

Key Takeaways from FTC Settlement with Lenovo Over Pre-Installed "Man-in-the-Middle" Software

On September 5, 2017, the Federal Trade Commission ("FTC") announced that it had agreed to enter into a settlement with Lenovo Inc., which allegedly preloaded some of its computers with invasive software that compromised consumers' privacy and security protections. The settlement with Lenovo—one of the world's largest computer manufacturers—requires Lenovo to pay $3.5 million to state regulators, implement new internal programs and be subject to reporting requirements and compliance oversight for 20 years. Looking closely at the underlying violations and terms of the settlement, the Lenovo case offers several lessons for companies seeking to avoid the increasingly numerous regulatory pitfalls in the areas of privacy and cybersecurity.

Background

The FTC's complaint against Lenovo was based on the "VisualDiscovery" software that came preinstalled on Lenovo computers that were sold to consumers. The software was installed on hundreds of thousands of computers and allegedly interfered with how users' browsers interacted with websites, created serious security vulnerabilities, and accessed sensitive information without adequate notice or consent. Specifically, VisualDiscovery delivered pop-up ads from the company's retail partners whenever a user's cursor hovered over a link for a similar product. To facilitate this, the software acted as a "man-in-the-middle" between a user's browser and the websites that the user visited, which provided it with access to sensitive information. If a user visited websites that required login credentials, Social Security numbers, payment information, or any other personal details, that data could be accessed by VisualDiscovery without the user's consent. Although only a limited amount of information was actually transmitted by VisualDiscovery to its parent company, the FTC noted that the company could choose to collect far more.

In addition to the actual and potential violation of users' privacy, VisualDiscovery created security risks. To facilitate pop-up ads on encrypted sites, the software used an insecure method to replace digital certificates with its own VisualDiscovery-signed certificates. As a result, a user's browser would verify the validity of the replacement certificate regardless of whether the original certificate was valid. The software thus allowed users to browse an insecure or spoofed website without their browsers providing any warning. In addition to rendering critical browser security functions useless, the VisualDiscovery-signed certificates all used the same private encryption key and easy-to-crack password on every laptop. A hacker who cracked the password on one laptop could therefore target every other laptop with VisualDiscovery installed and collect all of the personal information accessible to the software.

Based on these issues, the FTC issued a complaint against Lenovo alleging that its failure to take reasonable measures to assess and address the security risks posed by VisualDiscovery was an unfair act that caused or was likely to cause substantial injury to consumers. The complaint further alleged that Lenovo failed to make adequate disclosures about VisualDiscovery to users. The software came pre-installed and only displayed a one-time pop-up window the first time a user visited a shopping website. This pop-up informed users that their browsers were enabled with VisualDiscovery and included a small opt-out link at the bottom. According to the FTC, this did not

provide users with adequate notice that the software could access such a wide range of personal information and therefore users did not have the opportunity to provide informed consent.

Lenovo's settlement with the FTC and 32 state attorneys general has several provisions and requirements. Notably, Lenovo is: (1) prohibited from making misrepresentations about preinstalled software; (2) required to obtain a user's affirmative express consent before software like VisualDiscovery can act as a "man-in-the-middle;" (3) required to implement a software security program to address the security risks of preinstalled software and undergo software security assessments by a third party; and (4) required to comply with standard reporting and compliance provisions. The settlement remains in effect for 20 years, and Lenovo is further responsible for paying states approximately $3.5 million.

Lessons from *Lenovo*

As with any FTC action, the Lenovo settlement provides a trove of lessons for companies seeking to avoid unfair practices:

1. **Companies must provide users with clear notice and must obtain their affirmative consent before monitoring user activity or collecting personal information**. Here, the FTC noted that preinstalling invasive software and then providing a single, discreet opportunity to opt out was insufficient. While this may seem obvious in retrospect, companies should always ensure that they conspicuously notify their users what information they are seeking to access, obtain informed consent before accessing personal information, and honor user requests to revoke consent.

2. **Companies must provide and uphold digital security**. Here, Lenovo preinstalled software that accessed sensitive user information was easily hackable and undermined browser security functions. By focusing on this aspect of the case, the FTC is signaling that it is not just concerned about what information is being collected and used, but how information is being protected. It is not enough for companies to ensure that the software and services they provide to customers are secure—they must also ensure that their software and services do not compromise the security features of other programs.

3. **Companies may be held responsible for the acts and omissions of their vendors and affiliates**. Here, the FTC imputed responsibility to Lenovo for failing to identify, investigate and remedy the security issues caused by its vendor's VisualDiscovery software. Because liability may extend beyond a vendor to the company that purchases its products or services, companies should conduct an appropriate review of its vendors and products before and after deployment. Companies should conduct appropriate due diligence, insert appropriate contractual requirements and exercise reasonable oversight designed to uphold end user privacy and security.

More thoughts about the Lenovo settlement can be found on the FTC website, including a blog post highlighting additional lessons, available **here**.

September 6, 2017

Tracy L. Lechner
Shareholder
tlechner@bhfs.com
303.223.1274

Esteban M. Morin
Associate
emorin@bhfs.com
303.223.1275

This document is intended to provide you with general information regarding the FTC's recent settlement with Lenovo. The contents of this document are not intended to provide specific legal advice. If you have any questions about the contents of this document or if you need legal advice as to an issue, please contact your regular Brownstein Hyatt Farber Schreck, LLP attorney. This communication may be considered advertising in some jurisdictions.