152 3134

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

Commissioners: Maureen K. Ohlhausen, Acting Chairman
Terrell McSweeny

In the Matter of	)	
	)	**Docket No. C-4636**
LENOVO (UNITED STATES) INC.	)	
a corporation.	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that Lenovo (United States) Inc. has violated Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Lenovo (United States) Inc. ("Lenovo") is a Delaware corporation with its principal office or place of business located at 1009 Think Place, Morrisville, North Carolina 27560-9002.

2. The acts and practices of Respondent alleged in the Complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT'S BUSINESS PRACTICES

3. Respondent is one of the world's largest manufacturers of personal computers, including desktop computers, laptops, notebooks, and tablets. Respondent employs approximately 7,500 people in the United States.

4. In August 2014, Respondent began selling certain laptop models to U.S. consumers with a preinstalled ad-injecting software (commonly referred to as "adware"), known as VisualDiscovery. VisualDiscovery was developed by Superfish, Inc. , a Delaware corporation with its principal office or place of business located in Palo Alto, California.

5. VisualDiscovery delivered pop-up ads to consumers of similar-looking products sold by Superfish's retail partners whenever a consumer's cursor hovered over the image of a product on a shopping website. For example, if a consumer's cursor hovered over a product image while the consumer viewed owl pendants on a shopping website like Amazon.com, VisualDiscovery would overlay pop-up ads onto that website of other similar-looking owl pendants sold by Superfish's retail partners.

6. VisualDiscovery also operated as a local proxy that stood between the consumer's browser and all the Internet websites that the consumer visited, including encrypted https:// websites (commonly referred to as a "man-in-the-middle" or a "man-in-the-middle" technique). This man-in-the-middle technique allowed VisualDiscovery to see all of a consumer's sensitive personal information that was transmitted on the Internet, such as login credentials, Social Security numbers, financial account information, medical information, and web-based email communications. VisualDiscovery then collected, transmitted to Superfish servers, and stored a more limited subset of user information, including: the URL visited by the consumer; the text appearing alongside images appearing on shopping websites; the name of the merchant website being browsed; the consumer's IP address; and a unique identifier assigned by Superfish to the user's laptop (collectively, "consumer Internet browsing data"). Superfish had the ability to collect additional information from Lenovo users through VisualDiscovery at any time.

THE PREINSTALLATION OF VISUALDISCOVERY ON LENOVO LAPTOPS

7. VisualDiscovery is a Lenovo-customized version of Superfish's ad-injecting software, WindowShopper. During the course of discussions with Superfish, Lenovo required a number of modifications to Superfish's WindowShopper program. The most significant modification resulted from Lenovo's requirement that the software inject pop-up ads on multiple Internet browsers, including browsers that the consumer installed after purchase. This condition required WindowShopper to change the way it delivered ads.

8. To provide Respondent's required functionality, Superfish licensed and incorporated a tool from Komodia, Inc. With this tool, VisualDiscovery operated on every Internet browser installed on consumers' laptops, and injected pop-up ads on both http:// and encrypted https:// websites.

9. To facilitate its injection of pop-up ads into encrypted https:// connections, VisualDiscovery replaced the digital certificates for https:// websites visited by consumers with Superfish's own certificates for those websites. Digital certificates, part of the Transport Layer Security (TLS) protocol, are electronic credentials presented by https:// websites to consumers' browsers that, when properly validated, serve as proof that consumers are communicating with the authentic website and not an imposter.

10. VisualDiscovery was able to replace the websites' digital certificates because it installed a self-signed root certificate in the laptop's operating system, which caused consumers' browsers to automatically trust the VisualDiscovery-signed certificates. This allowed VisualDiscovery to act as a man-in-the-middle, causing both the browser and the website to believe that they had established a direct, encrypted connection, when in fact, the VisualDiscovery software was decrypting and re-encrypting all encrypted communications passing between them without the consumer's or the website's knowledge.

11. Superfish informed Respondent of its use of the Komodia tool and warned that it might cause antivirus companies to flag or block the software. And in fact, as discussed *infra* at Paragraphs 20-24, the modified VisualDiscovery software (using the Komodia tool) created two significant security vulnerabilities that put consumers' personal information at risk of unauthorized access. Without requesting or reviewing any further information, Lenovo approved Superfish's use of the Komodia tool.

12. After a security researcher reported to Respondent that there were problems with VisualDiscovery's interactions with https:// websites in September 2014, Respondent began to preinstall a second version of VisualDiscovery in December 2014 that did not operate on https:// websites or contain the root certificate that created the security vulnerabilities discussed *infra*. Respondent did not update laptops that had the original version of VisualDiscovery preinstalled or stop the shipment of those laptops. In total, over 750,000 U.S. consumers purchased a Lenovo laptop with VisualDiscovery preinstalled, with over half of those consumers purchasing laptops with the original version of VisualDiscovery preinstalled.

RESPONDENT'S DISCLOSURES ABOUT VISUALDISCOVERY'S PREINSTALLATION AND OPERATION WERE INADEQUATE

13. Respondent did not make any disclosures about VisualDiscovery to consumers prior to purchase. It did not disclose the name of the program; the fact that the program would act as a man-in-the-middle between consumers and all websites with which they communicated, including sensitive communications with encrypted https:// websites; or the fact that the program would collect and transmit consumer Internet browsing data to Superfish.

14. The VisualDiscovery software was designed to have limited visibility on the consumer's laptop. For example, the software was always on and running in the background without the consumer having to do anything to start or otherwise activate the software. There was no desktop icon for VisualDiscovery; there was no icon in the computer's applications tray to indicate that VisualDiscovery was running; and VisualDiscovery was not listed among the 'All Programs' list of installed programs, available when the consumer clicked on the Windows' Start button. The software was only visible on the laptop if consumers navigated to the Control Panel, where consumers could uninstall the program through Windows' 'Add/Remove' feature.

15. After consumers had purchased their laptops, VisualDiscovery displayed a one-time pop-up window the first time consumers visited a shopping website. Respondent worked with Superfish to customize the language of this pop-up window for its users. This pop-up stated:

> Explore shopping with VisualDiscovery: Your browser is enabled with VisualDiscovery which lets you discover visually similar products and best prices while you shop.

The pop-up window also contained a small opt-out link at the bottom of the pop-up that was easy for consumers to miss. If a consumer clicked on the pop-up's 'x' close button, or anywhere else on the screen, the consumer was opted in to the software. An example of the initial pop-up window is attached as Exhibit A.

16. The initial pop-up window failed to disclose, or failed to disclose adequately that VisualDiscovery would act as a man-in-the-middle between consumers and all websites with which they communicated, including sensitive communications with encrypted https:// websites, and collect and transmit consumer Internet browsing data to Superfish. These facts would be material to consumers in their decision of whether or not to use VisualDiscovery.

17. The omitted information was not available to consumers from other sources. VisualDiscovery's Privacy Policy and End User License Agreement (EULA), available via hyperlinks in the initial pop-up window, similarly omitted the material information.

18. Even if consumers saw and clicked on the opt-out link, the opt-out was ineffective. Clicking on the link would only stop VisualDiscovery from displaying pop-up ads; the software still acted as a man-in-the-middle between consumers and all websites with which they communicated, including sensitive communications with encrypted https:// websites.

VISUALDISCOVERY CREATED SECURITY VULNERABILITIES THAT PUT CONSUMERS' PERSONAL INFORMATION AT RISK OF UNAUTHORIZED ACCESS

19. VisualDiscovery's substitution of websites' digital certificates with its own certificates created two security vulnerabilities related to the TLS protocol. The TLS protocol uses digital certificates that, when properly validated, serve as proof that consumers are communicating with the authentic https:// website. When a user connects to a website with an invalid certificate, the browser will warn the user that the connection is untrusted. An untrusted connection indicates that unknown parties could intercept any information sent over that connection or that the endpoint of the connection may not be the website the consumer intended to visit.

20. Here, however, VisualDiscovery did not adequately verify that websites' digital certificates were valid before replacing them with its own certificates, which were automatically trusted by consumers' browsers. This caused consumers to not receive warning messages from their browsers if they visited potentially spoofed or malicious websites with invalid digital certificates, and rendered a critical security feature of modern web browsers useless.

21. VisualDiscovery created an additional security vulnerability because it used a self-signed root certificate that employed the same private encryption key, with the same easy-to-crack password ("komodia") on every laptop, rather than employing private keys unique to each laptop. This practice violated basic encryption key management principles

because attackers could exploit this vulnerability to issue fraudulent digital certificates that would be trusted by consumers' browsers. Not only was the password easy to crack – security researchers did so in less than hour – but once attackers had cracked the password on one consumer's laptop, they could target every Lenovo user with VisualDiscovery preinstalled with man-in-the-middle attacks that could intercept consumers' electronic communications with any website, including those for financial institutions and medical providers. Such attacks would provide attackers with unauthorized access to consumers' sensitive personal information, such as Social Security numbers, financial account numbers, login credentials, medical information, and email communications. This vulnerability also made it easier for attackers to deceive consumers into downloading malware onto any affected Lenovo laptop.

22. The risk that this vulnerability would be exploited increased after February 19, 2015, when security researchers published information about both vulnerabilities and bloggers described how to exploit the private encryption key vulnerability. The next day, on February 20, 2015, the United States Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security responsible for analyzing and reducing cyber threats and vulnerabilities, issued a public warning about the VisualDiscovery security vulnerabilities. US-CERT recommended that consumers remove VisualDiscovery with a free removal tool offered by Respondent that would also remove its root certificate. Many consumers spent considerable time removing VisualDiscovery and its root certificate from their affected laptops. Merely opting out, disabling, or uninstalling VisualDiscovery would not address the security vulnerabilities.

23. Respondent stopped shipping laptops with VisualDiscovery preinstalled on or about February 20, 2015, although some of these laptops, including laptops with the original version of VisualDiscovery preinstalled, were still being sold through various retail channels as late as June 2015.

RESPONDENT FAILED TO IMPLEMENT REASONABLE SECURITY REVIEWS OF ITS CUSTOMIZED VISUALDISCOVERY SOFTWARE

24. Respondent failed to take reasonable measures to assess and address security risks created by third-party software preinstalled on its laptops. For example,

    a. Respondent failed to adopt and implement written data security standards, policies, procedures or practices that applied to third-party software preinstalled on its laptops;

    b. Respondent failed to adequately assess the data security risks of third-party software prior to preinstallation;

    c. Respondent did not request or review any information about Superfish's data security policies, procedures and practices, including any security testing conducted by or on behalf of Superfish during its software development process, nor did Respondent request or review any information about the Komodia tool

after Superfish informed Respondent that it could cause VisualDiscovery to be flagged by antivirus companies;

d. Respondent failed to require Superfish by contract to adopt and implement reasonable data security measures to protect Lenovo users' personal information;

e. Respondent failed to assess VisualDiscovery's compliance with reasonable data security standards, including failing to reasonably test, audit, assess or review the security of VisualDiscovery prior to preinstallation; and

f. Respondent did not provide adequate data security training for those employees responsible for testing third-party software.

25. As a result of these security failures, Respondent did not discover VisualDiscovery's significant security vulnerabilities, as described above. Respondent could have discovered the VisualDiscovery security vulnerabilities prior to preinstallation by implementing readily available and relatively low-cost security measures.

26. Consumers had no way of independently knowing about Respondents' security failures and could not reasonably have avoided possible harms from such failures.

RESPONDENT'S PREINSTALLATION OF VISUALDISCOVERY HARMED CONSUMERS

27. VisualDiscovery harmed consumers with respect to accessing the Internet. Accessing the Internet, including for private, encrypted communications, represents a central use of consumer laptops.

28. VisualDiscovery prevented consumers from having the benefit of basic security features provided by their Internet browsers for encrypted https:// connections, as described above. The non-profit Electronic Frontier Foundation (EFF) found that affected Lenovo laptop users who participated in its SSL Observatory research project visited websites with invalid certificates, but did not receive warnings from their browsers that the potentially malicious websites they visited were improperly authenticated. Some consumers have also complained that they suffered from fraudulent bank account and credit card activity within months of buying their affected Lenovo laptops.

29. VisualDiscovery also caused many websites to load slowly, render improperly, or not load at all. According to a test conducted by Superfish on an affected Lenovo laptop, VisualDiscovery slowed Internet upload speeds by approximately 125 percent and download speeds by almost 25 percent. In one noted incident, a consumer could not use his Lenovo laptop to log onto his employer's Virtual Private Network (VPN) because the employer's network did not recognize the Superfish digital certificate.

30. These harms are not outweighed by countervailing benefits to consumers or competition, and are not reasonably avoidable by consumers.

FTC ACT VIOLATIONS

Count One – Deceptive Failure to Disclose

31. As alleged in Paragraphs 13-18, Respondent represented, directly or indirectly, expressly or by implication, to consumers that VisualDiscovery was enabled on their browser and would allow consumers to discover similar looking products with the best prices.

32. Respondent's representation failed to disclose, or failed to disclose adequately, that VisualDiscovery would act as a man-in-the-middle between consumers and all websites with which communicated, including sensitive communications with encrypted https:// websites, and collect and transmit consumer Internet browsing data to Superfish, as alleged in Paragraph 6.

33. Respondent's failure to disclose the material information described in Paragraph 32, in light of the representation set forth in Paragraph 31, was, and is, a deceptive act or practice.

34. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

Count Two – Unfair Preinstallation of Man-in-the-Middle Software

35. As alleged in Paragraphs 13-18, 27 and 29-30, Respondent's preinstallation of ad-injecting software that, without adequate notice or informed consent, acted as a man-in-the-middle between consumers and all the websites with which they communicated, including sensitive encrypted https:// websites, and collected and transmitted consumer Internet browsing data to Superfish, caused or is likely to cause substantial injury to consumers, that is not offset by countervailing benefits to consumers or competition, and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

36. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

Count Three – Unfair Security Practices

37. As alleged in Paragraphs 19-29, Respondent's failure to take reasonable measures to assess and address security risks created by third-party software preinstalled on its laptops, caused or is likely to cause substantial injury to consumers, that is not offset by countervailing benefits to consumers or competition, and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

38. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this twentieth day of December, 2017, has issued this complaint against Respondent.

By the Commission.

Donald S. Clark
Secretary

SEAL: