152 3134

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

Commissioners: Maureen K. Ohlhausen, Acting Chairman

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 0.001 Thp(t)-2c -0.a[(th)2(e)3(eb)1(s) 2(s

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 interaction 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.

The pop-up window also contained a small opt-

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 an in-the-middle attack that could intercept consumers' electronic communications with any website, including those of financial institutions and medical providers. Such attacks would provide attackers with unauthorized access to consumers' sensitive personal information, such as Socia

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

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 browsers 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 they 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 an 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 12-29, 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.