

COPY

[EXEMPT FROM FILING FEES  
UNDER GOVT. CODE, § 6103]

1 XAVIER BECERRA  
Attorney General of California  
2 NICKLAS A. AKERS  
Senior Assistant Attorney General  
3 STACEY D. SCHESSER  
Supervising Deputy Attorney General  
4 LISA B. KIM  
Deputy Attorney General  
5 State Bar No. 229369  
6 300 South Spring Street, Suite 1702  
7 Los Angeles, CA 90013  
Telephone: (213) 897-0013  
8 Fax: (213) 897-4951  
E-mail: Lisa.Kim@doj.ca.gov  
9 *Attorneys for Plaintiff*  
10 *The People of the State of California*

CONFORMED COPY  
ORIGINAL FILED  
Superior Court of California  
County of Los Angeles

SEP 05 2017

Sherri R. Carter, ~~Clerk~~ Officer/Clerk  
By: M. Soto, Deputy  
Moses Soto

11 SUPERIOR COURT OF THE STATE OF CALIFORNIA  
12 COUNTY OF LOS ANGELES

14 **PEOPLE OF THE STATE OF  
15 CALIFORNIA,**

16 Plaintiff,

17 v.

18 **LENOVO (UNITED STATES) INC., a  
19 corporation**

20 Defendant.

Case No. **BC 674647**

**COMPLAINT FOR INJUNCTIVE AND  
OTHER RELIEF**

(BUS. & PROF. CODE, § 17200 et seq.)

23 **COMPLAINT FOR INJUNCTIVE AND OTHER RELIEF**

24 1. Plaintiff, the People of the State of California, by Xavier Becerra, Attorney  
25 General of the State of California, ("Plaintiff" or "the People") brings this action against  
26 Defendant Lenovo (United States) Inc. ("Lenovo" or "Defendant") for violating the  
27  
28

1 California Unfair Competition Law (Bus. & Prof. Code § 17200 *et seq.*), and alleges the  
2 following on information and belief.

3 **JURISDICTION AND VENUE**

4 2. Defendant has transacted business within the State of California, including  
5 in the County of Los Angeles, at all times relevant to this complaint. The violations of law  
6 described herein occurred in the County of Los Angeles and elsewhere in the State of  
7 California.

8 **DEFENDANT**

9 3. Defendant Lenovo is a Delaware corporation with its principal place of  
10 business at 1009 Think Place, Morrisville, North Carolina 27560-9002.

11 **BACKGROUND**

12 4. In August 2014, Lenovo began selling certain laptop models to U.S.  
13 consumers with a preinstalled ad-injecting software (commonly referred to as “adware”),  
14 known as VisualDiscovery. VisualDiscovery was developed by Superfish, Inc.

15 5. VisualDiscovery operated as a purported shopping assistant by delivering  
16 pop-up ads to consumers of similar-looking products sold by Superfish’s retail partners  
17 whenever a consumer’s cursor hovered over the image of a product on a shopping website.  
18 If a consumer’s cursor hovered over a product image while the consumer viewed a  
19 particular style of lamp, for example, on a shopping website like Amazon.com,  
20 VisualDiscovery would inject pop-up ads onto that website of other similar-looking lamps  
21 sold by Superfish’s retail partners.

22 6. VisualDiscovery also operated as a local proxy that stood between the  
23 consumer’s browser and all the Internet websites that the consumer visited, including  
24 encrypted https:// websites (commonly referred to as a “man-in-the-middle” or a “man-in-  
25 the-middle” technique). This technique allowed VisualDiscovery to see all of a consumer’s  
26 sensitive personal information that was transmitted on the Internet. VisualDiscovery then  
27 collected, transmitted to Superfish servers, and stored a more limited subset of user  
28 information.

1           7.       VisualDiscovery is a Lenovo-customized version of an earlier Superfish ad-  
2 injecting software known as WindowShopper. During the course of discussions with  
3 Superfish, Lenovo required a number of modifications to WindowShopper, including the  
4 requirement that the software inject pop-up ads on multiple Internet browsers. This  
5 condition required Superfish to modify the manner in which the software delivered ads. To  
6 that end, Superfish licensed and incorporated a tool from Komodia, Inc., which allowed  
7 VisualDiscovery to operate on every Internet browser installed on consumers' laptops,  
8 including browsers installed after purchase, and inject pop-up ads on both http:// and  
9 encrypted https:// websites.

10           8.       To facilitate its injection of pop-up ads into encrypted https:// connections,  
11 VisualDiscovery installed a self-signed root certificate in the laptop's operating system that  
12 caused consumers' browsers to automatically trust the VisualDiscovery-signed certificates.  
13 This allowed VisualDiscovery to act as a man-in-the-middle, causing both the browser and  
14 the website to believe that they had established a direct, encrypted connection, when in fact,  
15 the VisualDiscovery software was decrypting and re-encrypting all encrypted  
16 communications passing between them without the consumer's or the website's knowledge.

17           9.       During the course of developing VisualDiscovery, Superfish informed  
18 Lenovo of its use of the Komodia tool and warned that it might cause antivirus companies  
19 to flag or block the software. In fact, the Komodia tool used in the modified  
20 VisualDiscovery software created significant security vulnerabilities that put consumers'  
21 personal information at risk of unauthorized access. Lenovo approved Superfish's use of  
22 the Komodia tool without requesting or reviewing any further information.

23           10.      In September 2014, Lenovo became aware that there were problems with  
24 VisualDiscovery's interactions with https:// websites relating to its use of a self-signed root  
25 certificate. Although Lenovo required Superfish to modify VisualDiscovery as a result, it  
26 failed to update laptops that had the original version of VisualDiscovery preinstalled or stop  
27 the shipment of those laptops. In total, over 750,000 U.S. consumers purchased a Lenovo  
28 laptop with VisualDiscovery preinstalled.

1           11.     Lenovo did not make any disclosures about VisualDiscovery to consumers  
2 prior to purchase, and such disclosures were not included in VisualDiscovery's Privacy  
3 Policy and End User License Agreement, or via hyperlinks in the initial pop-up window. It  
4 did not disclose the name of the program; the fact that the program would inject pop-up ads  
5 during the consumer's Internet browsing; the fact that the program would act as a man-in-  
6 the-middle between consumers and all websites with which they communicated, including  
7 sensitive communications with encrypted https:// websites; or the fact that the program  
8 would collect and transmit consumer Internet browsing data to Superfish. Further,  
9 VisualDiscovery was designed to have limited visibility on the consumer's laptop.

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

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

17           13.     The pop-up window also contained a small opt-out link at the bottom of the  
18 pop-up that was easy for consumers to miss. If a consumer clicked on the pop-up's 'x'  
19 close button, or anywhere else on the screen, the consumer was opted in to the software.

20           14.     Lenovo knew or should have known that this information was material to  
21 consumers. For example, prior to preinstalling VisualDiscovery, Lenovo knew of the  
22 existence of specific negative online consumer complaints about WindowShopper, the  
23 precursor to VisualDiscovery. Due to these negative reviews, Lenovo asked Superfish to  
24 rebrand its customized version of the WindowShopper program with a new name before  
25 Lenovo preinstalled it.

26           15.     Even if consumers saw and clicked on the opt-out link, the opt-out was  
27 ineffective. Clicking on the link would only stop VisualDiscovery from displaying pop-up  
28 ads; the software still acted as a man-in-the-middle between consumers and all websites

1 with which they communicated, including sensitive communications, with encrypted  
2 https:// websites.

3  
4 16. VisualDiscovery's substitution of websites' digital certificates with its own  
5 certificates created two security vulnerabilities. First, VisualDiscovery did not adequately  
6 verify that websites' digital certificates were valid before replacing them with its own  
7 certificates, which were automatically trusted by consumers' browsers. This caused  
8 consumers to not receive warning messages from their browsers if they visited potentially  
9 spoofed or malicious websites with invalid digital certificates, and rendered a critical  
10 security feature of modern web browsers useless.

11 17. Second, VisualDiscovery used a self-signed root certificate that employed  
12 the same private encryption key, with the same easy-to-crack password ("komodia") on  
13 every laptop, rather than employing private keys unique to each laptop. This practice  
14 violated basic encryption key management principles because attackers could exploit this  
15 vulnerability to issue fraudulent digital certificates that would be trusted by consumers'  
16 browsers and could provide attackers with unauthorized access to consumers' sensitive  
17 personal information.

18 18. The risk that this vulnerability would be exploited increased after February  
19 19, 2015, when security researchers published information about both vulnerabilities and  
20 bloggers described how to exploit the private encryption key vulnerability.

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

25 20. Lenovo failed to take reasonable measures to assess and address security  
26 risks created by third-party software preinstalled on its laptops. For example:  
27  
28

- a. Lenovo failed to adopt and implement written data security standards, policies, procedures or practices that applied to third-party software preinstalled on its laptops;
- b. Lenovo failed to adequately assess the data security risks of third-party software prior to preinstallation;
- c. Lenovo 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 Lenovo request or review any information about the Komodia tool after Superfish informed Lenovo that it could cause VisualDiscovery to be flagged by antivirus companies;
- d. Lenovo failed to require Superfish by contract to adopt and implement reasonable data security measures to protect Lenovo users' personal information;
- e. Lenovo 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. Lenovo did not provide adequate data security training for those employees responsible for testing third-party software.

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

22. VisualDiscovery harmed consumers and impaired the performance of their laptops in several ways, particularly with respect to accessing the Internet. Accessing the Internet, including for private, encrypted communications, represents a central use of consumer laptops.



- 1 c. Failing to follow reasonable security and privacy protocols with respect  
2 to software provided by third-party vendors that was to be preloaded  
3 onto Lenovo personal computers; and  
4 d. Failing to provide an easy way to remove or opt out of preinstalled  
5 software.

6 **PRAYER FOR RELIEF**

7 WHEREFORE, the People pray for judgment as follows:

8 A. Pursuant to Business and Professions Code section 17203, that Lenovo, its  
9 successors, agents, representatives, employees, and all persons and entities, corporate or  
10 otherwise, who act in concert with any of them, be permanently enjoined from engaging in unfair  
11 competition as defined in Business and Professions Code section 17200, including, but not  
12 limited to, the acts and practices alleged in this Complaint;

13 B. Pursuant to Business and Professions Code section 17203, that the Court make  
14 such orders or judgments as necessary to restore to any person in interest any money or property  
15 that may have been acquired by means of such unfair competition;

16 C. Pursuant to Business and Professions Code section 17206, that the Court assess a  
17 civil penalty of \$2,500 for each violation of Business and Professions Code section 17200, as  
18 proved at trial.

19 D. That Plaintiff recover its costs of suit, including costs of investigation;

20 E. For such other and further relief as the Court deems just and proper.

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

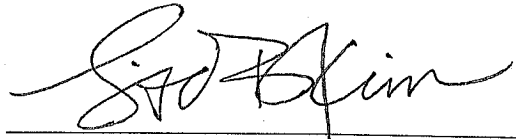
28 ///



1 Dated: September 5, 2017

Respectfully Submitted,

XAVIER BECERRA  
Attorney General of California  
NICKLAS A. AKERS  
Senior Assistant Attorney General  
STACEY SCHESSER  
Supervising Deputy Attorney General

6  
7 

8 LISA B. KIM  
9 Deputy Attorney General  
10 *Attorneys for Plaintiff,*  
11 *The People of the State of California*

11 SF2015102458  
12 52487795\_4.doc

13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28