

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

IN THE MATTER OF

COMMONWEALTH OF PENNSYLVANIA
OFFICE OF ATTORNEY GENERAL

PLAINTIFF

v.

LENOVO (UNITED STATES) INC.

DEFENDANT

Case No.

387 MD 2017

RECEIVED
COMMONWEALTH COURT
OF PENNSYLVANIA
2017 SEP -5 AM 10:06

NOTICE TO DEFEND

YOU HAVE BEEN SUED IN COURT. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you.

YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE.
IF YOU DO NOT HAVE A LAWYER, GO TO OR TELEPHONE THE

OFFICE SET FORTH BELOW. THIS OFFICE CAN PROVIDE YOU WITH INFORMATION ABOUT HIRING A LAWYER. IF YOU CANNOT AFFORD TO HIRE A LAWYER, THIS OFFICE MAY BE ABLE TO PROVIDE YOU WITH INFORMATION ABOUT AGENCIES THAT MAY OFFER LEGAL SERVICES TO ELIGIBLE PERSONS AT A REDUCED FEE OR NO FEE.

MIDPENN LEGAL SERVICES
213-A NORTH FRONT STREET
HARRISBURG, PENNSYLVANIA 17101
717-232-0581

DAUPHIN COUNTY LAWYER REFERRAL SERVICE
213 N. FRONT STREET
HARRISBURG, PENNSYLVANIA 17101
717-232-7536

IN THE MATTER OF

COMMONWEALTH OF PENNSYLVANIA
OFFICE OF ATTORNEY GENERAL

PLAINTIFF

V.

LENOVO (UNITED STATES) INC.

DEFENDANT

Case No. _____

COMPLAINT

AND NOW, comes the Commonwealth of Pennsylvania, acting by Attorney General Josh Shapiro, through the Bureau of Consumer Protection (“Commonwealth” or “Plaintiff”), and brings this action against Lenovo (United States) Inc. (“Lenovo” or “Defendant”) pursuant to the Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1, *et seq.* (“Consumer Protection Law”), to restrain unfair methods of competition or unfair or deceptive acts or practices in the conduct of any trade or commerce declared unlawful by Section 201-3 of the Consumer Protection Law. In support of this action the Commonwealth respectfully represents the following:

JURISDICTION AND VENUE

1. This Court has jurisdiction over this action pursuant to Section 761 of the Judicial Code, 42 P.S. § 761 and venue is proper pursuant to Pa.R.C.P. Nos. 1006(a)(1) and 2179(a)(2).

THE PARTIES

2. Plaintiff is the Commonwealth of Pennsylvania, acting by Attorney General Josh Shapiro, through the Bureau of Consumer Protection, with its office located at 15th Floor, Strawberry Square, Harrisburg, Pennsylvania 17120.

3. Defendant is a Delaware corporation with its principal place of business at 1009 Think Place, Morrisville, North Carolina 27560-9002. Defendant registered with the Pennsylvania Department of State as a foreign business corporation effective March 2005.

BACKGROUND

4. Lenovo has engaged in and continues to engage in trade and commerce within the Commonwealth of Pennsylvania by manufacturing, advertising, offering for sale, and selling personal computers, including desktop computers, laptops, notebooks, and tablets.

5. In August 2014, Lenovo 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.

6. VisualDiscovery operated as a purported shopping assistant by delivering 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. If a consumer’s cursor hovered over a product image while the consumer viewed a particular style of lamp, for example, on a shopping website like Amazon.com, VisualDiscovery would inject pop-up ads onto that website of other similar-looking lamps sold by Superfish’s retail partners.

7. 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 technique allowed VisualDiscovery to see all of a consumer’s sensitive personal information that was transmitted on the Internet. VisualDiscovery then collected, transmitted to Superfish servers, and stored a more limited subset of user information.

8. VisualDiscovery is a Lenovo-customized version of an earlier Superfish ad-injecting software known as WindowShopper. During the course of discussions with Superfish, Lenovo required a number of modifications to WindowShopper, including the requirement that the software inject pop-up ads on

multiple Internet browsers. This condition required Lenovo to modify the manner in which the software delivered ads. To that end, Superfish licensed and incorporated a tool from Komodia, Inc., which allowed VisualDiscovery to operate on every Internet browser installed on consumers' laptops, including browsers installed after purchase, and inject pop-up ads on both http:// and encrypted https:// websites.

9. To facilitate its injection of pop-up ads into encrypted https:// connections, VisualDiscovery installed a self-signed root certificate in the laptop's operating system that 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.

10. During the course of developing VisualDiscovery, Superfish informed Lenovo of its use of the Komodia tool and warned that it might cause antivirus companies to flag or block the software. In fact, the Komodia tool used in the modified VisualDiscovery software created significant security vulnerabilities that put consumers' personal information at risk of unauthorized access. Lenovo

approved Superfish's use of the Komodia tool without requesting or reviewing any further information.

11. In September 2014, Lenovo became aware that there were problems with VisualDiscovery's interactions with <https://> websites relating to its use of a self-signed root certificate. Although Lenovo required Superfish to modify VisualDiscovery as a result, it failed to 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.

12. Lenovo did not make any disclosures about VisualDiscovery to consumers prior to purchase, and such disclosures were not included in VisualDiscovery's Privacy Policy and End User License Agreement, or via hyperlinks in the initial pop-up window. It did not disclose the name of the program; the fact that the program would inject pop-up ads during the consumer's Internet browsing; 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. Further, VisualDiscovery was designed to have limited visibility on the consumer's laptop.

13. After consumers had purchased their laptops, VisualDiscovery displayed a one-time pop-up window the first time consumers visited a shopping website. Lenovo 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.

14. 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.

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

16. 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.

17. VisualDiscovery's substitution of websites' digital certificates with its own certificates created two security vulnerabilities. First, 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.

18. Second, VisualDiscovery 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 and could provide attackers with unauthorized access to consumers' sensitive personal information.

19. 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.

20. Lenovo 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.

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

- (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.

22. 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.

23. 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.

24. VisualDiscovery prevented consumers from having the benefit of basic security features provided by their Internet browsers for encrypted https:// connections, as described above. VisualDiscovery also disrupted consumers' Internet browsing experience by causing pop-up ads to block content on websites visited by consumers, and caused many websites to load slowly, render improperly, or not load at all.

VIOLATIONS OF THE CONSUMER PROTECTION LAW

25. The preceding paragraphs are incorporated herein by reference as if the same were fully set forth.

26. Lenovo, in the course of manufacturing, advertising, offering for sale, and selling computers, has engaged in business acts or practices that are unfair or deceptive methods, acts, or practice as prohibited by Section 201-3 of the Consumer Protection Law by:

- (a) Failing to disclose to consumers prior to purchase that VisualDiscovery was preloaded onto certain models of Lenovo's products;
- (b) Failing to disclose, or failing to disclose adequately, that VisualDiscovery would: (i) cause consumers to receive unlimited pop-up ads whenever their cursor hovered over a product image on a shopping website that would disrupt consumers' Internet browsing experience; (ii) cause many websites to load slowly, render improperly, or not load at all; and (iii) 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;
- (c) Failing to take reasonable measures to assess and address security risks created by third-party software preinstalled on its laptops; and
- (d) Failing to provide an easy way to remove or opt out of preinstalled software.

27. The following acts and practices constitute unfair methods of competition and/or unfair or deceptive acts or practices as prohibited by Section 201-3 of the Consumer Protection Law, including, without limitation:

- (a) Passing off goods or services as those of another, in violation of 73 P.S. § 201-2(4)(i);

- (b) Causing likelihood of confusion or of misunderstanding as to the source, sponsorship, approval or certification of goods or services, in violation of 73 P.S. § 201-2(4)(ii);
- (c) Causing likelihood of confusion or of misunderstanding as to affiliation, connection or association with, or certification by, another, in violation of 73 P.S. § 201-2(4)(iii);
- (d) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that he does not have, in violation of 73 P.S. § 201-2(4)(v); and
- (e) Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding, in violation of 73 P.S. § 201-2(4)(xxi).

28. Said conduct is willful and is unlawful under Section 201-3 of the Consumer Protection Law. 73 P.S. § 201-3.

PRAYER FOR RELIEF

WHEREFORE, the Commonwealth respectfully requests this Honorable Court to issue an Order:

A. Declaring Defendant's conduct as described in the Complaint to be in violation of the Consumer Protection Law.

B. Requiring Defendant, pursuant to Section 201-8(b) of the Consumer Protection Law, to pay civil penalties in the amount of One Thousand Dollars (\$1,000.00) for each and every violation of the Consumer Protection Law and

Three Thousand Dollars (\$3,000.00) for each violation involving a victim age sixty (60) or older.

C. Requiring Defendant to pay the Commonwealth for the cost of investigation and prosecution of this action.

D. Directing the Defendant to disgorge and forfeit all profits they have derived as a result of their unfair and deceptive acts and practices as set forth in this Complaint.

E. Permanently enjoining Defendant, their agents, successors, assigns and employees acting directly or through any corporate device, from engaging in the aforementioned acts, practices, methods of competition or any other practice in violation of the Consumer Protection Law.

F. Granting such other and further relief as the Court deems just, proper, and equitable under the circumstances.

Respectfully Submitted,

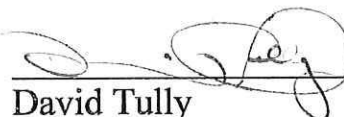
COMMONWEALTH OF PENNSYLVANIA
OFFICE OF ATTORNEY GENERAL

JOSH SHAPIRO
ATTORNEY GENERAL

Date: 9/05/17 By: Nicole DiTomo
Nicole R. DiTomo
Deputy Attorney General
PA Attorney I.D. No. 315325
Bureau of Consumer Protection
15th Floor, Strawberry Square
Harrisburg, Pennsylvania 17120
Telephone: (717) 705-6559
Email: nditomo@attorneygeneral.gov

VERIFICATION

I, David Tully, being duly sworn according to law, hereby state that I am in excess of eighteen (18) years of age and that I am an Agent for the Office of Attorney General, Bureau of Consumer Protection and that I am authorized to make this verification that the facts set forth in the foregoing Complaint are true and correct to the best of my knowledge or information and belief.

Date: 9/05/17 By: 
David Tully
Consumer Protection Agent