COMPB
ADAM PAUL LAXALT
Attorney General
LUCAS J. TUCKER (Bar No. 010252)
Senior Deputy Attorney General
LAURA M. TUCKER (Bar No. 13268)
Deputy Attorney General
State of Nevada
Office of the Attorney General
10791 W. Twain Avenue, #100
Las Vegas, Nevada 89135
702-486-3256 ph / 702-486-3283 fax
ltucker@ag.nv.gov
lmtucker@ag.nv.gov
Attorneys for Plaintiff, State of Nevada

DISTRICT COURT
CLARK COUNTY, NEVADA

STATE OF NEVADA, Plaintiff, vs. LENOVO (UNITED STATES) INC. Defendant.	CASE NO. : DEPT. NO.: **BUSINESS COURT REQUESTED** **ARBITRATION EXEMPTION—** **Action in Equity**

COMPLAINT

Plaintiff, the STATE OF NEVADA, by and through ADAM PAUL LAXALT, Attorney General of the State of Nevada, and his deputies, Senior Deputy Lucas Tucker and Deputy Laura Tucker, brings this action against Lenovo (United States) Inc. (hereinafter "Lenovo" or "Defendant") in the public interest pursuant to Nevada Deceptive Trade Practice Act, NRS 598.0903 et seq., ("NV Deceptive Trade Act") to protect consumers from unlawful deceptive business practices.

JURISDICTION AND VENUE

1. This action is brought for and on behalf of the STATE of NEVADA, by ADAM PAUL LAXALT, Attorney General of the State of Nevada, pursuant to the provisions of the NV Deceptive Trade Act, NRS 598.0903 et seq.

2. This Court has jurisdiction over the Defendant pursuant to NRS 598.0963 and 598.0999, because Defendant has transacted business within the State of Nevada or has engaged in conduct impacting Nevada and its consumers at all times relevant to this complaint.

3. Venue for this action properly lies in the Eighth Judicial District Court, Clark County, Nevada, pursuant to NRS 598.0989(3) as Defendant transacted business in the State of Nevada and the deceptive trade practices alleged herein occurred in Clark County, Nevada.

THE PARTIES

4. Plaintiff, the STATE OF NEVADA (hereinafter "the State"), is represented by ADAM PAUL LAXALT, Attorney General of the State of Nevada, who is charged, inter alia, with the enforcement of the NV Deceptive Trade Act, NRS 598.0903 et seq., and authorized to bring this action pursuant to NRS 598.0963.

5. Defendant is a Delaware corporation that has been qualified to conduct business in Nevada since its filing with the Nevada Secretary of State on March 2, 2005, and has its principal place of business at 1009 Think Place, Morrisville, North Carolina 27560-9002.

FACTUAL BACKGROUND

6. Lenovo has engaged in and continues to engage in trade and commerce within the State of Nevada by manufacturing, advertising, offering for sale, and selling personal computers, including desktop computers, laptops, notebooks, and tablets. Lenovo employs approximately 7,500 people in the United States.

7. 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.

8. 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 inject pop-up ads onto that website of other similar-looking owl pendants sold by Superfish's retail partners.

9. 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. 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").

10. 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.

11. This condition required Superfish 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.

12. 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.

13. 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.

14. Superfish informed Lenovo of its use of the Komodia tool and warned that it might cause antivirus companies to flag or block the software. Without requesting or reviewing any further information, Lenovo approved Superfish's use of the Komodia tool.

15. After a security researcher reported to Lenovo that there were problems with VisualDiscovery's interactions with https:// websites in September 2014, Lenovo 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*. Lenovo 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, including Nevada consumers, purchased a Lenovo laptop with VisualDiscovery preinstalled.

16. Lenovo affirmatively disclosed to consumers only some of the software that was included on its computers prior to purchase. Those disclosures included the operating system (*i.e.*, Windows Operating Systems) and certain software, such as McAfee security software, and internet browsers.

17. Lenovo 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 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.

18. VisualDiscovery was designed to have limited visibility on the consumer's laptop. The software was only readily visible on the laptop if consumers navigated to the Control Panel, where consumers could uninstall the program through Windows' 'Add/Remove' feature.

19. 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.

20. 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.

21. The initial pop-up window failed to disclose, or failed to disclose adequately, facts about VisualDiscovery that would be material to consumers in their decision of whether or not to use VisualDiscovery, including unlimited pop-up ads that would disrupt consumers' Internet browsing experience, slow internet performance, and the collection and transmission of consumer Internet browsing data to Superfish. This material information was similarly omitted from VisualDiscovery's Privacy Policy and End User License Agreement, available via hyperlinks in the initial pop-up window.

22. 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.

23. 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.

24. 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.

25. 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. This vulnerability also made it easier for attackers to deceive consumers into downloading malware onto any affected Lenovo laptop.

26. 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. 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.

27. 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.

28. 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.

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

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

31. 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.

32. 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.

//

//

CAUSES OF ACTION

COUNT I

Violations of the NV Deceptive Trade Practices Act
NRS 598.0903 et seq.

33. Plaintiff re-alleges the facts above and incorporates them herein by reference.

34. As alleged herein, Lenovo, in the course of business engaged in deceptive practices in violation of the NV Deceptive Trade Act in that it used deception, deceptive practices and/or misrepresentations and omissions in the course of manufacturing, advertising, offering for sale, and selling computers.

35. Defendant's deceptive conduct constitutes multiple violations of the NV Deceptive Trade Act, including but not limited to:

(a) NRS 598.0915(2), a person engages in a deceptive trade practice by knowingly making a false representation as to the certification of goods for sale or lease;

(b) NRS 598.0915(3), a person engages in a deceptive trade practice by knowingly making a false representation as to certification by another person;

(c) NRS 598.0915(5), a person engages in deceptive trade practice by knowingly making a false representation as to the characteristics, uses or benefits of goods or services for sale or lease;

(d) NRS 598.0915(7), a person engages in a deceptive trade practice by representing that goods or services for sale or lease are of a particular standard, quality or grade, if he or she knows or should know that they are of another standard, quality or grade;

(e) NRS598.0915(9), a person engages in a deceptive trade practice by advertising goods or services with intent not to sell or lease them as advertised; and

(f) NRS 598.0923(2), a person engages in a deceptive trade practice by failing to disclose a material fact in connection with the sale or lease of goods or services.

36. In all matters alleged herein, the Defendant acted in the course of its business or occupation within the meaning NRS 598.0903 to 598.0999.

37. In all requisite matters alleged herein, the Defendant acted knowingly within the meaning of NRS 598.0903 to 598.0999.

38. In all matters alleged herein, the Defendant acted willfully in violation of NRS 598.0903 et seq., as required for the imposition of penalties under NRS 598.0999(2).

PRAYER FOR RELIEF

WHEREFORE, the State respectfully requests that the Court:

A. Enter an order permanently enjoining the Defendant from continuing the unlawful acts and practices alleged in this Complaint or doing any acts in furtherance of such unlawful acts or practices;

B. Enter an order requiring the Defendant to pay a civil penalty in an amount not to exceed $5,000 per violation for all violations of the NV Deceptive Trade Act, pursuant to NRS 598.0999(2);

C. Enter an order requiring the Defendant to pay a civil penalty in an amount not to exceed $12,500 per violation found by the Court to have been directed toward an elderly or disabled person, pursuant to NRS 598.0973;

D. Enter an order directing the Defendant to disgorge all revenues, profits and gains achieved in whole or in part through the unfair and/or deceptive acts or practices complained herein;

//

//

//

//

//

E. Enter an order requiring the Defendant to pay costs and expenses of this action incurred by the Attorney General, including but not limited to, attorney's fees and costs pursuant to NRS 598.0999(2); and

F. Order any such further relief as this Court may deem just and proper.

Dated this 5th day of September 2017.

Respectfully submitted,

ADAM PAUL LAXALT
Attorney General

By: _____
LUCAS J. TUCKER (Bar No. 010252)
Senior Deputy Attorney General
LAURA M. TUCKER (Bar No. 13268)
Deputy Attorney General