CHRISTOPHER S. PORRINO
ATTORNEY GENERAL OF NEW JERSEY
Division of Law
124 Halsey Street - 5th Floor
P.O. Box 45029
Newark, New Jersey 07101
Attorney for the Plaintiffs

By: Elliott M. Siebers – ID# 033582012
Deputy Attorneys General

SUPERIOR COURT OF NEW JERSEY
CHANCERY DIVISION, MERCER COUNTY
DOCKET NO. _____

CHRISTOPHER S. PORRINO, Attorney General of the State of New Jersey, and SHARON M. JOYCE, Acting Director of the New Jersey Division of Consumer Affairs, Plaintiffs, v. Lenovo, Inc. Defendant.	Civil Action **COMPLAINT**

Plaintiffs, Christopher S. Porrino, Attorney General of the State of New Jersey ("Attorney General"), with offices located at 124 Halsey Street, Fifth Floor, Newark, New Jersey, and Sharon M. Joyce, Acting Director of the New Jersey Division of Consumer Affairs ("Director"), with offices located at 124 Halsey Street, Seventh Floor, Newark, New Jersey (collectively, "Plaintiffs"), by way of Complaint state:

JURISDICTION AND VENUE

1. The Attorney General is charged with the responsibility of enforcing the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 et seq. ("CFA"). The Director is charged with the responsibility of administering the CFA on behalf of the Attorney General.

2. Venue is proper in Mercer County, pursuant to R. 4:3-2, because it is a county in which Lenovo conducted business.

THE PARTIES

1. Plaintiffs, Christopher S. Porrino, Attorney General of the State of New Jersey ("Attorney General"), with offices located at 124 Halsey Street, Fifth Floor, Newark, New Jersey, and Sharon M. Joyce, Acting Director of the New Jersey Division of Consumer Affairs ("Director"), with offices located at 124 Halsey Street, Seventh Floor, Newark, New Jersey (collectively, "Plaintiffs"), by way of Complaint state:

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

BACKGROUND

3. Lenovo has engaged in and continues to engage in trade and commerce within the State of New Jersey 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.

4. 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.

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 inject pop-up ads onto that website of other similar-looking owl pendants sold by Superfish's retail partners. VisualDiscovery displayed its pop-up ads without the website owner's permission or knowledge, and without paying the website owner any of the advertising revenues generated.

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 Lenovo'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 Lenovo 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 22 through 26, 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 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 purchased a Lenovo laptop with VisualDiscovery preinstalled.

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

13. 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.

14. 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 consumers' 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.

15. VisualDiscovery was designed to have limited visibility on a 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 readily visible on the laptop if consumers navigated to the Control Panel, where consumers could uninstall the program through Windows' "Add/Remove" feature.

16. 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.

17. 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.

18. The initial pop-up window failed to disclose, or failed to disclose adequately that VisualDiscovery would: (a) 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; (b) cause many websites to load slowly, render improperly, or not

load at all; and (c) 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.

19. 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.

20. Lenovo knew or should have known that this information was material to consumers. For example, prior to preinstalling VisualDiscovery, Lenovo knew that consumers often viewed adware as "junk," and that there were specific online consumer complaints about WindowShopper, the precursor to VisualDiscovery. These complaints described WindowShopper as malware and expressed frustration with its intrusiveness. Due to these negative online consumer reviews, Lenovo asked Superfish to rebrand its customized version of the WindowShopper program with a new name before Lenovo preinstalled it.

21. 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

22. 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.

23. 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.

24. 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.

25. 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 Lenovo 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.

26. 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.

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

27. 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.

28. 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.

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

LENOVO'S PREINSTALLATION OF VISUALDISCOVERY HARMED CONSUMERS

30. 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.

31. 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.

32. VisualDiscovery also disrupted consumers' Internet browsing experience. The software's pop-up ads blocked content on websites visited by consumers, and required consumers to interrupt their browsing to click on the 'x' close button to remove the pop-up ads. VisualDiscovery ads did not "time out" or close if a consumer clicked elsewhere on the screen. There was also no limit on the number of pop-up ads shown to a consumer; rather, the software displayed pop-up ads every time a consumer's cursor hovered over a product image on a shopping website. Consumer complaints regarding their poor user experience with VisualDiscovery were so significant that Lenovo decided to stop its preinstallation of VisualDiscovery, in part, because of these complaints.

33. 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.

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

COUNT I
VIOLATIONS OF THE CFA
(UNCONSCIONABLE COMMERCIAL PRACTICES)

35. Plaintiffs repeat and re-allege the allegations contained in paragraphs 1 through 34 above as if more fully set forth herein.

36. The CFA, N.J.S.A. 56:8-2, prohibits:

> The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise . . .

37. The CFA defines "merchandise" as "any objects, wares, goods commodities, services or anything offered, directly or indirectly to the public for sale." N.J.S.A. 56:8-1(c).

38. At all relevant times, Lenovo has engaged in the advertisement, offer for sale and/or sale of merchandise within the meaning of N.J.S.A. 56:8-1(c).

40. Lenovo, in the course of advertising, offering for sale, and selling computers to the public, has engaged in unconscionable commercial practices prohibited by the CFA, N.J.S.A. 56:8-2 including, but not limited to:

a. Failing to follow reasonable security and privacy protocols with respect to software provided by third-party vendors that was to be preloaded onto Lenovo personal computers; and

b. Preinstalling VisualDiscovery software that 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 provide an easy way for consumers to remove or opt out of preinstalled software.

41. Each unconscionable commercial practice by Lenovo constitutes a separate violation under the CFA, N.J.S.A. 56:8-2.

COUNT II

VIOLATIONS OF THE CFA (DECEPTIVE ACTS OR PRACTICES)

42. Plaintiffs restate and re-allege paragraphs 1-34 of this Complaint

43. Lenovo, in the course of advertising, offering for sale, and selling computers to the public, has engaged in deceptive acts or practices prohibited by the CFA, N.J.S.A. 56:8-2, including, without limitation:

a. 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 consumers communicated, including sensitive communications with encrypted https:// websites, and collect and transmit consumer Internet browsing data to Superfish;

b. Affirmatively representing that its personal computers contained certain software programs (*i.e.*, Windows Operating System, McAfee security software, internet browsers, etc.) that consumers believed were of a certain quality, when in actuality, its pre-installation of VisualDiscovery so undermined and compromised the software that they functioned in an inferior manner.

44. Each deceptive act or practice by Lenovo constitutes a separate violation under the CFA, N.J.S.A. 56:8-2.

PRAYER FOR RELIEF

WHEREFORE, the Plaintiffs respectfully request this Honorable Court to issue an Order:

I. Declaring Defendant's conduct as described in the Complaint to be in violation of the CFA;

II. Assessing civil penalties against Defendants for each and every violation of the CFA pursuant to N.J.S.A. 56:8-13;

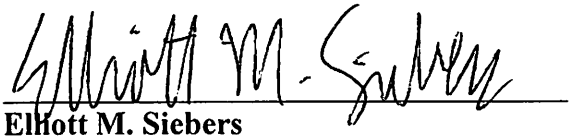
III. Permanently enjoining Defendants their agents, successors, assigns and employees acting directly or through any corporate device, from engaging in any acts or practices in

violation of the CFA, N.J.S.A. 56:8-1 et seq., , including, but not limited to, the acts and practices alleged in the Complaint;

IV. Assessing investigative costs and fees, including attorneys' fees, against Defendants for the use of the State of New Jersey, as authorized by the CFA, N.J.S.A. 56:8-11 and N.J.S.A. 56:8-19.

Respectfully Submitted,

CHRISTOPHER S. PORRINO
ATTORNEY GENERAL OF NEW JERSEY
Attorney for Plaintiff Division of Consumer Affairs

Date: Sept. 5, 2017 By: 

Elliott M. Siebers
Deputy Attorney General
Attorney I.D. No. 033582012
Affirmative Civil Enforcement Practice Group
124 Halsey Street, 5th Floor
Newark, New Jersey 07302
Telephone: (973) 648-4460
Facsimile: (973) 648-4887
Email: elliott.siebers@law.njoag.gov