DOCKET NO.	:	RETURN DATE: 9/19/17
STATE OF CONNECTICUT	:	SUPERIOR COURT
	:	
Plaintiff	:	JUDICIAL DISTRICT OF
	:	HARTFORD
v.	:	
	:	
LENOVO (UNITED STATES) INC.	:	
	:	SEPTEMBER 5, 2017
Defendant	:	

COMPLAINT

This is an action pursuant to the Connecticut Unfair Trade Practices Act ("CUTPA"), Chapter 735a of the Connecticut General Statutes, more specifically Conn. Gen. Stat. § 42-110m, to secure injunctive relief against the defendant Lenovo (USA) Inc., which alleges unfair or deceptive acts and practices which violate Conn. Gen. Stat. § 42-110b, to obtain relief as is necessary to redress injury to consumers resulting from the defendant's violations of law, to obtain appropriate equitable relief, and for civil penalties.

THE PARTIES

1.   The Plaintiff is the State of Connecticut (the "State" or the "Plaintiff"), represented by George Jepsen, Attorney General of the State of Connecticut, acting at the request of Michelle Seagull, Commissioner of Consumer Protection, pursuant to Conn. Gen. Stat. § 42-110m(a).

2.   The defendant Lenovo (United States) Inc. ("Lenovo" or the "Defendant") is a Delaware corporation with its principal place of business at 1009 Think Place, Morrisville, North Carolina 27560-9002.

BACKGROUND

3.   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.

4.   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.

5.   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.

6.   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 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

2

Internet browser installed on consumers' laptops, including browsers installed after purchase, and inject pop-up ads on both http:// and encrypted https:// websites.

7.   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.

8.   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.

9.   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.

10.   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.

11.   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.

12.   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.

13.   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.

14.   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.

15.   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.

16.   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.

17.   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.

18.   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.

19.   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.

20.   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.

21.   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.

22.   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 CUTPA

23.   CUTPA at § 42-110b(a) states the following: "[n]o person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."

24.   CUTPA states at § 42-110a(4): "trade" and "commerce" shall mean the "advertising, the sale or rent or lease, the offering for sale or lease, or the distribution of any service or any property, tangible or intangible, real, personal or mixed, and any article, commodity, or thing of value in this state."

25.   CUTPA also states at § 42-110b(b) that: "[i]t is the intent that in construing subsection (a) of this section, the commissioner and the courts of this state shall be guided by interpretations given by the Federal Trade Commission and the federal courts to Section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. § 45(a)(1)), as from time to time amended."

26.   Lenovo manufactures personal computers that are sold in retail stores in the State. Lenovo also maintains a website through which consumers can purchase Lenovo products and ship those products to consumers residing in the State.

27.   Lenovo therefore has engaged in trade or commerce in the State of Connecticut.

COUNT I

Deceptive Failure to Disclose

1-27.   The allegations of Paragraphs 1 through 27 are incorporated by reference as Paragraphs 1-27 of Count I as if fully set forth herein.

28.   Lenovo failed to make any disclosures to consumers prior to purchase that VisualDiscovery was preloaded onto certain models of Lenovo's products.

29.   Specifically, Lenovo 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.

30.   Defendant's failure to disclose the material information described in paragraphs 1-27, in light of the allegations set forth in paragraph 10, was likely to mislead consumers acting reasonably under the circumstances.

31.   Defendant's failure to disclose, as set forth in this Count, was material to consumers' decisions about whether or not to purchase Lenovo products preinstalled with VisualDiscovery.

32.   Defendant has therefore engaged in unfair or deceptive acts and practices in violation of Conn. Gen. Stat. § 42-110b(a).

<center>**COUNT II**</center>

<center>**Civil Penalties – Deceptive Failure to Disclose**</center>

1-27.   The allegations of Paragraphs 1 through 27 are incorporated by reference as Paragraphs 1 through 27 of Count II as if fully set forth herein.

28.   Defendant engaged in the acts and practices alleged herein when they knew or should have known that their conduct was unfair or deceptive, in violation of Conn. Gen. Stat. § 42-110b(a), and, therefore, are liable for civil penalties of up to $5,000 per willful violation pursuant to Conn. Gen. Stat. § 42-110o(b).

<center>**COUNT III**</center>

<center>**Unfair Failure to Follow Reasonable Security Practices**</center>

1-27.   The allegations of Paragraphs 1 through 27 are incorporated by reference as Paragraphs 1 through 27 of Count III as if fully set forth herein.

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

29.   Lenovo's failure to take reasonable measures to assess and address security risks created by third-party software preinstalled on its laptops violated the public policy set forth in Conn. Gen. Stat. § 42-471, which requires persons in possession of personal information of another person to safeguard the data, computer files and documents containing the information from misuse by third parties.

30.   The Defendant's course of conduct as alleged herein was unethical, immoral, oppressive, and unscrupulous.

31.   The Defendant's course of conduct as alleged herein caused substantial injury to consumers which could not have been reasonably avoided and which produced no countervailing benefits.

32.   The Defendant's acts and practices as alleged herein therefore constitute unfair or deceptive acts or practices in violation of General Statutes § 42-110b(a).

COUNT IV

Civil Penalties – Unfair Failure to Follow Reasonable Security Practices

1-27.   The allegations of Paragraphs 1 through 27 are incorporated by reference as Paragraphs 1 through 27 of Count IV as if fully set forth herein.

28.   Defendant engaged in the acts and practices alleged herein when they knew or should have known that their conduct was unfair or deceptive, in violation of Conn. Gen. Stat. §42-110b(a), and, therefore, are liable for civil penalties of up to $5,000 per willful violation pursuant to Conn. Gen. Stat. § 42-110o(b).

WHEREFORE, the Plaintiff claims the following relief:

An order, pursuant to General Statutes § 42-110m(a), enjoining the Defendants from further violation of General Statutes § 42-110b(a).

An order, pursuant to General Statutes § 42-110m(a), directing the Defendants to pay restitution.

An order, pursuant to General Statutes § 42-110m(a), directing the Defendants to notify those of its customers who may have been a victim of the acts and practices described herein of the availability of restitution.

An order, pursuant to General Statutes § 42-110o(b), directing the Defendants to pay civil penalties for each willful violation of General Statutes § 42-110b(a).

An order, pursuant to General Statutes § 42-110m(a), directing the Defendants to disgorge all revenues, profits and gains achieved in whole or in part through the unfair and/or deceptive acts or practices complained of herein.

An accounting, pursuant to General Statutes § 42-110m(a) to determine the amounts properly owed to those of its customers who may have been a victim of the acts and practices described herein.

An award of attorneys fees, pursuant to General Statutes § 42-110m(a).

Costs of suit.

Such other and further relief as the Court deems appropriate.

The Plaintiff hereby states that the amount in demand is more than Fifteen Thousand Dollars ($15,000.00), exclusive of interest and costs.

HEREOF FAIL NOT, BUT OF THIS WRIT, MAKE DUE SERVICE AND RETURN, ACCORDING TO LAW.

Dated at Hartford, Connecticut, this 5th day of September, 2017.

PLAINTIFF
STATE OF CONNECTICUT
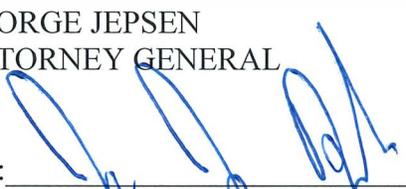
GEORGE JEPSEN
ATTORNEY GENERAL

BY:_____
Jonathan J. Blake (Juris No. 426816)
Matthew F. Fitzsimmons (Juris. No. 426834)
Assistant Attorneys General
Office of the Attorney General
McKenzie Hall
110 Sherman Street
Hartford, Connecticut 06105
Tel: (860) 808-5400
Jonathan.blake@ct.gov
Matthew.fitzsimmons@ct.gov

DOCKET NO.   :   RETURN DATE: 9/19/17

STATE OF CONNECTICUT   :   SUPERIOR COURT
                                        :
    Plaintiff   :   JUDICIAL DISTRICT OF
                                        :   HARTFORD
    v.   :
                                        :
LENOVO (UNITED STATES) INC.   :
                                        :   SEPTEMBER 5, 2017
    Defendant   :

STIPULATED JUDGMENT

Plaintiff, the State of Connecticut (the "State"), represented by George Jepsen, Attorney General, acting at the request of Michelle Seagull, Commissioner of Consumer Protection, has filed a Complaint for a permanent injunction and other relief in this matter pursuant to the Connecticut Unfair Trade Practices Act (CUTPA), Conn. Gen. Stat. § 42-110b, *et seq.*, alleging Defendant, Lenovo (United States) Inc. ("Defendant" or "Lenovo," as defined in Part III of this Stipulated Judgment below), committed violations of CUTPA.

Plaintiff and Lenovo have agreed to the Court's entry of this Stipulated Judgment ("Stipulated Judgment") without trial or adjudication of any issue of fact or law or finding of wrongdoing or liability of any kind, and that Lenovo does not admit any violation of law or any wrongdoing. This Stipulated Judgment is for settlement purposes only, and it is the intent of the parties that, to the fullest extent permitted by law, neither the fact of, nor any provision contained in, this Stipulated Judgment, nor any action taken hereunder, shall constitute, be construed as, or be admissible in evidence as any admission of the validity of any claim or any fact alleged in any other pending or subsequently filed action or of any wrongdoing, fault, violation of law, or liability of any kind on the part of Lenovo or admission by Lenovo of the validity or lack thereof

1

of any claim, allegation, or defense asserted in any other action. Nothing in this Stipulated Judgment shall be construed to affect Lenovo's right to take legal or factual positions in defense of litigation or other legal proceedings to which the State is not a party.

I.   PARTIES

A.   Plaintiff is the State of Connecticut, represented by George Jepsen, Attorney General, acting at the request of Michelle Seagull, Commissioner of Consumer Protection.

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

II.   FINDINGS

A.   The Court has jurisdiction over the subject matter of the Complaint filed herein and, solely for the purposes of this matter, over the parties to this Stipulated Judgment. Jurisdiction is retained by this Court for the purpose of enabling Plaintiff to apply to this Court for such further orders and directions as may be necessary or appropriate for the construction, modification, or execution of this Stipulated Judgment, including the enforcement of compliance therewith and penalties for violation thereof.

B.   At all times relevant to this matter, Lenovo was engaged in trade and commerce affecting consumers in the State of Connecticut in that Lenovo manufactures personal computers that are sold in retail stores in the State. Lenovo also maintains a website through which consumers can purchase Lenovo products and ship those products to consumers residing in the State of Connecticut.

NOW THEREFORE, on the basis of these findings, and for the purpose of effecting this Stipulated Judgment, IT IS HEREBY ORDERED AND DECREED AS FOLLOWS:

III. DEFINITIONS

For purposes of this Stipulated Judgment, the following definitions apply:

A.   "Affirmative Express Consent" means that:

     i.   Prior to the initial operation of any Covered Software, it shall be Clearly and Conspicuously disclosed, separate and apart from any "end user license agreement," "privacy policy," "terms of use" page or similar document, the following:

        1. For any Covered Software that displays advertising,

          a.   The fact that the Covered Software will display advertisements, including any pop-up advertisements; and

          b.   The frequency and circumstances under which such advertisements are displayed to the consumer; and

        2. For any Covered Software that transmits, or causes to be transmitted, Covered Information to a person or entity other than the consumer,

          a.   The fact that the software will transmit, or cause to be transmitted, the Covered Information to a person or entity other than the consumer;

          b.   The types of Covered Information that will be transmitted to a person or entity other than the consumer;

          c.   The types of Covered Information that the receiving person or entity will share with third parties, which does not include an entity with a common corporate ownership and branding of Defendant or the

Software Provider, a Third Party Service Provider, or any person or entity otherwise excluded by the Proviso in Part IV.B of this Stipulated Judgment;

      d.   The identity or specific categories of such third parties; and

      e.   The purposes for sharing such Covered Information.

    ii.   At the time this disclosure is made, a Clear and Conspicuous mechanism shall be provided for a consumer to indicate assent to the operation of the Covered Software by taking affirmative action authorizing its operation.

B.   "Application Software" means any computer program designed for and used by consumers (e.g., database programs, word processing programs, games, Internet browsers or browser add-ons) that Defendant preinstalls or causes to be preinstalled onto a Covered Product. Application Software does not include device drivers; system software designed to configure, optimize or maintain a computer; operating systems; software bundled, integrated or included with operating systems; or software otherwise provided to Defendant for preinstallation on a Covered Product by an operating system provider.

C.   "Clear(ly) and Conspicuous(ly)" means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by consumers, including in all of the following ways:

    i.   In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be

presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure ("Triggering Representation") is made through only one means.

ii. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

iii. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for consumers to easily hear and understand it.

iv. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

v. On a product label, the disclosure must be presented on the principal display panel.

vi. The disclosure must use diction and syntax understandable to consumers and must appear in each language in which the Triggering Representation appears.

vii. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

viii. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

D.   "Covered Information" means the following information from or about an individual consumer that is input into, stored on, accessed or transmitted through Application Software: (a) a first and last name; (b) a physical address; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) login credentials and passwords; (e) a telephone number; (f) a Social Security number; (g) a driver's license or other government-issued identification number; (h) a financial institution account number; (i) credit or debit card information; (j) any portion of the content of a consumer's communications; (k) any portion of the content of a consumer's files (e.g., documents, photos or videos); and (l) precise geolocation information sufficient to identify a street name and name of a city or town.

E.   "Covered Product" means any personal computer (i.e., desktop computers, laptops, laptops that convert into tablets or vice versa, and notebooks) that is manufactured by or on behalf of Defendant and is sold to U.S. consumers. Covered Products do not include servers and server peripherals, mobile handsets or smartphones, or tablets or similar devices that are sold without an integrated or detachable physical keyboard. Covered Products also do not include the actual personal computers specifically sold to enterprise customers with over 1,000 employees.

F.   "Covered Software" means: (a) Application Software that injects advertisements into a consumer's Internet browsing session, including pop-up advertisements or (b) Application Software that transmits, or causes to be transmitted, Covered Information to a person or entity other than the consumer, except when

i.   the Covered Information is used only in an aggregated and/or de-identified form that does not disclose, report, or otherwise share any individually identifiable information; or

ii.   the Covered Information is transmitted or used solely for one or more of the following purposes:

1. being reasonably necessary for the software to perform a function or service that the consumer requests or otherwise interacts with;

2. authenticating the consumer;

3. configuring or setting up the software; or

4. assessing or analyzing the software's performance (e.g., to find or fix problems in the software, assess how consumers are using the software, or to make improvements to the software).

Covered Software does not include Internet browsers, antivirus software, parental control software, or other computer security software.

G.   "Effective Date" of this Stipulated Judgment is the later of the date that the Court enters an Order, Judgment or Decree approving the terms of this document, or the effective date of the Order in the FTC Action.

H.   "Feature" means one or more of the following attributes of Covered Software: (a) the Covered Software's benefits, efficacy, or features; (b) the fact that it will display advertising, including pop-up advertisements; (c) the frequency and circumstances under which the Covered Software will display advertising; and (d) the fact of and extent to which the

Covered Software will transmit, or cause to be transmitted, Covered Information to a person or entity other than the consumer.

I.   "FTC Action" means the Federal Trade Commission matter entitled In re Matter of Lenovo (United States) Inc., File No. 152 3134.

J.   "Lenovo" or "Defendant" means Lenovo (United States) Inc. and its successors and assigns.

K.   "Participating States" or "States" refers to the states and commonwealths listed in Exhibit A.

L.   "Software Provider" means any person or entity other than Defendant that sells, leases, licenses, or otherwise provides Application Software.

M.   "Third Party Service Provider" means any person or entity that is contractually required by Defendant or a Software Provider to: (a) use or receive Covered Information collected by or on behalf of Defendant or the Software Provider for and at the direction of Defendant or Software Provider, and for no other individual or entity; (b) not disclose the Covered Information, or any individually identifiable information derived from it, to any individual or entity other than Defendant or Software Provider; and (c) not use the Covered Information for any other purpose.

IV.   INJUNCTIVE RELIEF

A.   Prohibited Misleading Representations

It is ordered that Defendant, its officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Stipulated Judgment, whether acting directly or indirectly, in connection with the advertising,

promotion, offering for sale, sale, or distribution of Covered Software shall not make a misrepresentation, in any manner, expressly or by implication, about any Feature of the Covered Software.

     B.   Affirmative Express Consent Provision

It is further ordered that, commencing no later than 120 days after the Effective Date of this Stipulated Judgment, Defendant, its officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Stipulated Judgment, whether acting directly or indirectly, shall not preinstall or cause to be preinstalled any Covered Software unless Defendant or the Software Provider:

     i.   Will obtain the consumer's Affirmative Express Consent;

     ii.   Provides instructions for how the consumer may revoke consent to the Covered Software's operation, which can include uninstalling the Covered Software; and

     iii.   Provides a reasonable and effective means for consumers to opt out, disable or remove all of the Covered Software's operations, which can include uninstalling the Covered Software.

Provided, however, that Affirmative Express Consent will not be required if sharing the Covered Information is reasonably necessary to comply with applicable law, regulation or legal process.

     C.   Mandated Software Security Program

It is further ordered that Defendant must, no later than the Effective Date of this Stipulated Judgment, establish and implement, and thereafter maintain a comprehensive software security program that is reasonably designed to (1) address software security risks related to the

development and management of new and existing Application Software, and (2) protect the security, confidentiality, and integrity of Covered Information. The content, implementation and maintenance of the software security program must be fully documented in writing. The software security program must contain administrative, technical, and physical safeguards appropriate to Defendant's size and complexity, the nature and scope of Defendant's activities, the nature of the Application Software, the security policies and practices of the Software Provider, and the sensitivity of the Covered Information, including:

     i.   The designation of an employee or employees to coordinate and be responsible for the software security program;

     ii.   The identification of internal and external risks to the security, confidentiality, or integrity of Covered Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment must include consideration of risks in each area of relevant operation, including: (1) employee training and management; (2) Application Software design, including the processing, storage, transmission and disposal of Covered Information by the Application Software; and (3) the prevention, detection, and response to attacks, intrusions, or other vulnerabilities;

iii.   The design and implementation of reasonable safeguards to control these risks, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

iv.   The development and use of reasonable steps to select and retain software or service providers capable of maintaining security practices consistent with this Stipulated Judgment, and requiring software and service providers, by contract, to implement and maintain appropriate safeguards; and

v.   The evaluation and adjustment of the software security program in light of the results of the testing and monitoring required by sub-provision iii above, any changes to Defendant's operations or business arrangements, or any other circumstances that Defendant knows or has reason to know may have an impact on the effectiveness of the software security program.

D.   Software Security Assessments by a Third Party

It is further ordered that, in connection with compliance with the provision of this Stipulated Judgment titled Mandated Software Security Program, Defendant must obtain initial and biennial assessments ("Assessments"):

i.   The Assessments must be obtained from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A professional qualified to prepare such Assessments must be a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with professional experience

with secure Internet-accessible, consumer-grade devices; an individual qualified as a Certified Information Systems Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA) with professional experience with secure Internet-accessible consumer-grade devices; or a qualified individual or entity approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, as ordered in the FTC Action.

ii. The reporting period for the Assessments must cover: (1) the first 180 days after the Effective Date for the initial Assessment, and (2) each 2-year period thereafter for 20 years for the biennial Assessments.

iii. Each Assessment must:

1. Set forth the specific administrative, technical, and physical safeguards that Defendant has implemented and maintained during the reporting period;

2. Explain how such safeguards are appropriate to Defendant's size and complexity, the nature and scope of Defendant's activities, the nature of the Application Software, the security policies and practices of the Application Software provider and the sensitivity of the Covered Information;

3. Explain how the safeguards that have been implemented meet or exceed the protections required by the Provision of this Stipulated Judgment titled Mandated Software Security Program; and

4. Certify that the Mandated Software Security Program is operating with sufficient effectiveness to provide reasonable assurance that the security of the Application Software preinstalled on Covered Products and the security, confidentiality, and integrity of Covered Information is protected, and that the Mandated Software Security Program has so operated throughout the reporting period.

iv. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies as set forth in Part IV of the Order in the FTC Action.

E. The obligations and other provisions set forth in this Section IV shall expire 20 years after the Effective Date of this Stipulated Judgment. Nothing in this paragraph should be construed or applied to excuse Lenovo from its obligations to comply with all applicable state and federal laws, regulations and rules.

V. COMPLIANCE MONITORING

Defendant is required to monitor its compliance with this Stipulated Judgment in the same manner as it is required to monitor its compliance with the Order in the FTC Action, all as detailed in Part VI of the Order in the FTC Action. Upon request by any Participating State, Lenovo shall provide a copy of any Assessment or other submission made to the FTC pursuant to the FTC Action within 10 days of the request.

VI. ACKNOWLEDGEMENTS OF THE STIPULATED JUDGMENT

For 5 years after the Effective Date of this Stipulated Judgment, Defendant must deliver a copy of this Stipulated Judgment to all individuals and entities listed in Part V of the Order in the FTC Action.

VII. PAYMENT TO THE STATES

Within 30 days of the Effective Date Lenovo shall pay the State Two Hundred Eighty-Six Thousand One Hundred and Forty-Five Dollars ($286,145.00) pursuant to CUTPA. Of this sum, Eight Hundred Ninety and 97/100 Dollars ($890.97), representing the State's costs and expenses relating to this action, shall be deposited in the Consumer Fund of the Office of the Attorney General and the remaining **Two Hundred Eighty-Five Thousand Two Hundred and Fifty-Four and 3/100 Dollars ($285,254.03)** shall be deposited in the General Fund. Such payment shall be made by check payable to the "Treasurer, State of Connecticut," and shall be delivered to the Attorney General's Office, Privacy and Data Security Department, 110 Sherman Street, Hartford, Connecticut 06105, Attn: AAG Matthew F. Fitzsimmons, Department Head. Said sum paid to the State is made as part of a multistate settlement which includes a total payment of Three Million Five Hundred Thousand Dollars ($3,500,000) to the Participating States.

VIII. RELEASE

Following full payment of the amounts due under this Stipulated Judgment, the State shall release and discharge Lenovo and its affiliates, subsidiaries and divisions from all civil claims that the State could have brought under CUTPA based on Lenovo's conduct alleged in the Complaint filed in this matter prior to the Effective Date of this Stipulated Judgment. Nothing contained in this paragraph shall be construed to limit the ability of the State to enforce the

obligations that Lenovo has under this Stipulated Judgment. Further, nothing in this Stipulated Judgment shall be construed to create, waive, or limit any private right of action.

IX. GENERAL PROVISIONS

A. The Parties understand and agree that this Stipulated Judgment shall not be construed as an approval or a sanction by the State of Lenovo's business practices, nor shall Lenovo represent that this Stipulated Judgment constitutes an approval or sanction of its business practices. The Parties further understand and agree that any failure by the State to take any action in response to any information submitted pursuant to this Stipulated Judgment shall not be construed as an approval, waiver, or sanction of any representations, acts, or practices indicated by such information, nor shall it preclude action thereon at a later date, except as provided by the Release herein.

B. Nothing in this Stipulated Judgment shall be construed as relieving Lenovo of the obligation to comply with all state and federal laws, regulations, and rules, nor shall any of the provisions of this Stipulated Judgment be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

C. Nothing contained in this Stipulated Judgment shall be construed to waive or limit any right of action by any consumer, person or entity, or by any local, state, federal or other governmental entity, except as provided by the Release herein.

D. Nothing in this Stipulated Judgment shall prevent or restrict the use of this Stipulated Judgment by the State in any action against Lenovo for contempt or failure to comply with any of its provisions, or in the event that Lenovo is in default of any of its terms and conditions. A default on the part of Lenovo shall include any material breach by Defendant of

any of the terms or requirements of this Stipulated Judgment. Nothing in this Stipulated Judgment shall be construed to (i) exonerate any contempt or failure to comply with any of its provisions after the Effective Date of this Stipulated Judgment, (ii) compromise or limit the authority of the State to initiate a proceeding for any contempt or other sanctions for failure to comply, or (iii) compromise the authority of the Court or any other court of competent jurisdiction to punish as contempt any violation of this Stipulated Judgment.

E.   Those signing for Lenovo below hereby state that they each are authorized to enter into and execute this Stipulated Judgment by and on behalf of Lenovo.

F.   Lenovo further agrees to execute and deliver all authorizations, documents and instruments which are necessary to carry out the terms and conditions of this Stipulated Judgment, whether required prior to, contemporaneous with or subsequent to the Effective Date of this Stipulated Judgment, as defined herein.

G.   To the extent that there are any, Lenovo agrees to pay all court costs associated with the filing of this Stipulated Judgment. No court costs, if any, shall be taxed against the State.

H.   Lenovo shall not, directly or indirectly, participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices in whole or in part in the State that are prohibited by this Stipulated Judgment or for any other purpose that would otherwise circumvent any term of this Stipulated Judgment. Lenovo shall not cause, knowingly permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Stipulated Judgment.

I.   This Stipulated Judgment may be executed by any number of counterparts and by different signatories on separate counterparts, each of which shall constitute an original counterpart thereof and all of which together shall constitute one and the same document. One or more counterparts of this Stipulated Judgment may be delivered by facsimile or electronic transmission with the intent that it or they shall constitute an original counterpart thereof.

J.   This Stipulated Judgment sets forth all of the promises, covenants, agreements, conditions and understandings between the parties, and supersedes all prior and contemporaneous agreements, understandings, inducements or conditions, express or implied. There are no representations, arrangements, or understandings, oral or written, between the parties relating to the subject matter of this Stipulated Judgment that are not fully expressed herein or attached hereto. Each party specifically warrants that this Stipulated Judgment is executed without reliance upon any statement or representation by any other party hereto, except as expressly stated herein.

K.   Lenovo agrees that this Stipulated Judgment does not entitle it to seek or to obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and Lenovo further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

L.   This Stipulated Judgment shall not be construed to waive any claims of sovereign immunity the State may have in any action or proceeding.

M.   Except as otherwise provided under law, this Stipulated Judgment may only be enforced by the State, Lenovo, and this Court. The Parties to this action may agree, in writing, through counsel, to an extension of any time period in this Stipulated Judgment without a Court order.

X.   SEVERABILITY

If any clause, provision, or section of this Stipulated Judgment shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity or unenforceability shall not affect any other clause, provision or section of this Stipulated Judgment and this Stipulated Judgment shall be construed and enforced as if such illegal, invalid or unenforceable clause, section or provision had not been contained herein.

XI.   NOTICE/DELIVERY OF DOCUMENTS

Whenever Lenovo shall submit documents or provide notice to the State under this Stipulated Judgment, that requirement shall be satisfied by sending notice to: Designated Contacts on behalf of the Attorneys General listed in Exhibit A. Any notices or other documents sent to Lenovo pursuant to this Stipulated Judgment shall be sent to the following address: (1) Lenovo (United States) Inc., ATTN: General Counsel, 1009 Think Place, Morrisville, North Carolina 27560-900 and (2) Rebecca S. Engrav, Esq., Perkins Coie, 1201 Third Avenue, Suite 4900, Seattle, WA 98101-3099. All notices or other documents to be provided under this Stipulated Judgment shall be sent by United States mail, certified mail return receipt requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the notice or document, and shall have been deemed to be sent upon mailing. Any party may update its address by sending written notice to the other party.

PLAINTIFF
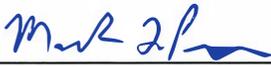STATE OF CONNECTICUT

GEORGE JEPSEN
ATTORNEY GENERAL

By: _____

Jonathan J. Blake (Juris No. 426816)
Matthew F. Fitzsimmons (Juris No. 426834)
Assistant Attorneys General
Office of the Attorney General
McKenzie Hall
110 Sherman Street
Hartford, Connecticut 06105
Tel.: (860) 808-5400
Fax: (860) 808-5593
Jonathan.blake@ct.gov
Matthew.fitzsimmons@ct.gov

DEFENDANT
LENOVO (UNITED STATES) INC.

By: _____

Christian Teismann
Senior Vice President and General Manager,
Lenovo North America Sales (Interim)

By: _____

Mark F. Parise (CT Juris No. 420944)
Perkins Coie LLP
30 Rockefeller Plaza, 22nd Floor
New York, New York 10112-0085
Tel.: 212-261-6890
Fax: 212-399-8090
MParise@perkinscoie.com
Local Counsel for Lenovo (United States) Inc.

Rebecca S. Engrav
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
Tel.: 206-359-6168
Fax: 206-359-7168
REngrav@perkinscoie.com
Lead Counsel for Lenovo (United States) Inc.

Entered:

_____   Date: _____

Judge

19

By: _____
Jonathan J. Blake (Juris No. 426816)
Matthew F. Fitzsimmons (Juris No. 426834)
Assistant Attorneys General
Office of the Attorney General
McKenzie Hall
110 Sherman Street
Hartford, Connecticut 06105
Tel.: (860) 808-5400
Fax: (860) 808-5593
Jonathan.blake@ct.gov
Matthew.fitzsimmons@ct.gov

DEFENDANT
LENOVO (UNITED STATES) INC.

By: _____
Christian Teismann
Senior Vice President and General Manager,
Lenovo North America Sales (Interim)

By: _____
Mark F. Parise (CT Juris No. 420944)
Perkins Coie LLP
30 Rockefeller Plaza, 22nd Floor
New York, New York 10112-0085
Tel.: 212-261-6890
Fax: 212-399-8090
MParise@perkinscoie.com
Local Counsel for Lenovo (United States) Inc.

Rebecca S. Engrav
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
Tel.: 206-359-6168
Fax: 206-359-7168
REngrav@perkinscoie.com
Lead Counsel for Lenovo (United States) Inc.

Entered:

_____   Date: _____
Judge

19

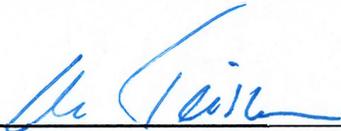By: _____

Jonathan J. Blake (Juris No. 426816)
Matthew F. Fitzsimmons (Juris No. 426834)
Assistant Attorneys General
Office of the Attorney General
McKenzie Hall
110 Sherman Street
Hartford, Connecticut 06105
Tel.: (860) 808-5400
Fax: (860) 808-5593
Jonathan.blake@ct.gov
Matthew.fitzsimmons@ct.gov

DEFENDANT
LENOVO (UNITED STATES) INC.

By: _____
Christian Teismann
Senior Vice President and General Manager,
Lenovo North America Sales (Interim)

By: _____
Mark F. Parise (CT Juris No. 420944)
Perkins Coie LLP
30 Rockefeller Plaza, 22nd Floor
New York, New York 10112-0085
Tel.: 212-261-6890
Fax: 212-399-8090
MParise@perkinscoie.com
Local Counsel for Lenovo (United States) Inc.

Rebecca S. Engrav
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
Tel.: 206-359-6168
Fax: 206-359-7168
REngrav@perkinscoie.com
Lead Counsel for Lenovo (United States) Inc.

Entered:

_____   Date: _____
Judge

19

Exhibit A

STATE	ATTORNEYS GENERAL DESIGNATED CONTACTS
Arizona	Taren Ellis Langford Unit Chief Counsel Arizona Attorney General's Office 400 W. Congress Street, Suite S-315 Tucson, AZ 85701 Taren.Langford@azag.gov (520) 628-6631
Arkansas	Peggy Johnson Assistant Attorney General Office of the Arkansas Attorney General 323 Center Street, Suite 500 Little Rock, Arkansas 72201 peggy.johnson@arkansasag.gov (501) 682-8062
California	Lisa B. Kim Deputy Attorney General Office of the Attorney General Consumer Law Section Privacy Enforcement and Protection Unit 300 South Spring Street, Suite 1702 Los Angeles, CA 90013 Lisa.Kim@doj.ca.gov (213) 897-0013
Colorado	Mark Bailey Senior Assistant Attorney General Colorado Attorney General's Office 1300 Broadway 7th Fl. Denver CO 80203 Mark.bailey@coag.gov (720) 508-6202
Connecticut	Matthew F. Fitzsimmons Assistant Attorney General Department Head Privacy and Data Security Department Office of the Attorney General 110 Sherman Street Hartford CT 06105 Matthew.Fitzsimmons@ct.gov (860) 808-5515

Exhibit A

Florida	Edward Moffitt Senior Financial Investigator/Supervisor Multistate & Privacy Bureau Office of the Attorney General 135 W Central Blvd, Suite 670 Orlando, FL 32801-2437 Edward.Moffitt@MyFloridaLegal.com (407) 845-6388
Hawaii	Lisa P. Tong Enforcement Attorney State of Hawaii Office of Consumer Protection 235 S. Beretania Street #801 Honolulu, Hawaii 96813 ltong@dcca.hawaii.gov (808) 586-5978
Idaho	Stephanie Guyon Deputy Attorney General Idaho Attorney General's Office Consumer Protection Division 954 W. Jefferson Street, 2nd FL. Boise, ID 83702 stephanie.guyon@ag.idaho.gov (208) 334-4135
Illinois	Matthew W. Van Hise, CIPP/US Assistant Attorney General Consumer Privacy Counsel Consumer Fraud Bureau Illinois Attorney General's Office 500 South Second Street Springfield, IL 62706 mvanhise@atg.state.il.us (217) 782-9024
Indiana	Ernâni Magalhães Deputy Attorney General Consumer Protection Division Office of Attorney General Curtis Hill 302 West Washington Street IGCS-5th Floor Indianapolis, IN 46204 ernani.magalhaes@atg.in.gov (317) 234-6681

Exhibit A

Iowa	Nathan Blake Assistant Attorney General Office of the Attorney General of Iowa 1305 E. Walnut St. Des Moines, IA 50319 nathan.blake@iowa.gov (515) 281-4325
Kansas	Sarah M. Dietz Assistant Attorney General Office of Kansas Attorney General Derek Schmidt 120 SW 10th Avenue, 2nd Floor sarah.dietz@ag.ks.gov (785) 296-3751
Louisiana	L. Christopher Styron Section Chief - Consumer Protection Assistant Attorney General Louisiana Department of Justice 1885 N. Third Street Baton Rouge, Louisiana 70802 styronl@ag.louisiana.gov (225) 326-6468
Maine	Linda Conti Assistant Attorney General Maine Office of the Attorney General 6 State House Station Augusta, Maine 04333-0006 Linda.conti@maine.gov (207) 626-8591
Minnesota	Evan Romanoff Assistant Attorney General Minnesota Attorney General's Office 445 Minnesota Street, Suite 1200 St. Paul, MN 55101 Evan.romanoff@ag.state.mn.us (651) 757-1454

Missouri	Joyce Yeager Assistant Attorney General Consumer Protection Section Office of the Missouri Attorney General PO Box 899 Jefferson City, MO 65102 joyce.yeager@ago.mo.gov (573) 751-6733
Nebraska	Daniel Birdsall Assistant Attorney General Consumer Protection Division Nebraska Attorney General's Office 2115 State Capitol Building Lincoln, NE 68509 dan.birdsall@nebraska.gov (402) 471-3840
Nevada	Nevada Consumer Advocate Office of the Nevada Attorney General Bureau of Consumer Protection 100 N. Carson St. Carson City, NV 89701 (775) 684-1100 aginfo@ag.nv.gov
New Hampshire	John W. Garrigan Assistant Attorney General Consumer Protection and Antitrust Bureau New Hampshire Department of Justice 33 Capitol Street Concord, NH 03301 603-271-1252 john.garrigan@doj.nh.gov
New Jersey	Elliott M. Siebers Deputy Attorney General Affirmative Civil Enforcement Practice Group Office of the Attorney General State of New Jersey 124 Halsey St. – 5th Floor P.O. Box 45029-5029 Newark, NJ 07101 elliott.siebers@law.njoag.gov (973) 648-4460

Exhibit A

New York	Clark Russell Deputy Bureau Chief Bureau of Internet and Technology New York State Office of the Attorney General 120 Broadway New York, NY 10271-0332 clark.russell@ag.ny.gov (212) 416-6494
North Carolina	Kim D'Arruda, CIPP/US Special Deputy Attorney General North Carolina Department of Justice Consumer Protection Division 114 West Edenton Street Raleigh, NC 27603 kdarruda@ncdoj.gov (919) 716-6013
North Dakota	Brian M. Card Assistant Attorney General Consumer Protection & Antitrust Division Office of Attorney General of North Dakota 1050 E. Interstate Ave., Suite 200 Bismarck, ND 58503-5574 bmcard@nd.gov (701) 328-5570
Oregon	Eva H. Novick Assistant Attorney General Financial Fraud/Consumer Protection Section Oregon Department of Justice 100 SW Market Street Portland, OR 97201 eva.h.novick@doj.state.or.us (971) 673-1880
Pennsylvania	John M. Abel, Esquire Pennsylvania Office of Attorney General Bureau of Consumer Protection 15th Floor, Strawberry Square Harrisburg, PA 17120 jabel@attorneygeneral.gov

Exhibit A

Rhode Island	Edmund F. Murray, Jr. Special Assistant Attorney General Rhode Island Department of Attorney General 150 South Main Street Providence, Rhode Island 02903 emurray@riag.ri.gov (401) 274-4400 ext. 2401
South Carolina	Chantelle L. Neese Assistant Attorney General SC Attorney General's Office Consumer Protection & Antitrust Section Rembert C. Dennis Bldg 1000 Assembly St. P. O. Box 11549 Columbia, SC 29211 CNeese@scag.gov (803) 734-2346
South Dakota	Philip D. Carlson Assistant Attorney General Consumer Protection Division South Dakota Attorney General 1302 E. Hwy. 14, Ste. 1 Pierre, SD 57501 Phil.Carlson@state.sd.us (605) 773-3216
Tennessee	Carolyn Smith Senior Counsel Consumer Protection and Advocate Division Tennessee Attorney General's Office P.O. Box 20207 Nashville, TN 37202-0207 carolyn.smith@ag.tn.gov (615) 532-2578
Texas	C. Brad Schuelke Senior Assistant Attorney General Office of the Attorney General Consumer Protection Division 300 W. 15th Street, 9th Floor Austin, Texas 78701 Brad.schuelke@oag.texas.gov (512) 463-1269

Exhibit A

Vermont	Ryan Kriger Assistant Attorney General Vermont Office of the Attorney General Public Protection Division 109 State St. Montpelier, VT 05609 ryan.kriger@vermont.gov (802) 828-3170
Washington	Andrea Alegrett Assistant Attorney General Office of the Attorney General, State of Washington 800 Fifth Avenue, Suite 2000 Seattle, WA 98104-3188 andreaa1@atg.wa.gov (206) 389-3813