

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Maureen K. Ohlhausen, Acting Chairman
Terrell McSweeney**

In the Matter of

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

DOCKET NO. C-4636

DECISION AND ORDER

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violation of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statement by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission’s Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondent is a Delaware corporation, with its principal office or place of business located at 1009 Think Place, Morrisville, North Carolina 27560-9002.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

- A. "Respondent" means Lenovo (United States) Inc., and its successors and assigns.
- B. "Affirmative express consent" means that:
 1. 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:
 - a. For any covered software that displays advertising,
 - i. the fact that the covered software will display advertisements, including any pop-up advertisements; and
 - ii. the frequency and circumstances under which such advertisements are displayed to the consumer; and
 - b. For any covered software that transmits, or causes to be transmitted, covered information to a person or entity other than the consumer,
 - i. the fact that the software will transmit, or cause to be transmitted, the covered information to a person or entity other than the consumer;
 - ii. the types of covered information that will be transmitted to a person or entity other than the consumer;

- iii. 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 Respondent or the software provider, a third party service provider, or any person or entity otherwise excluded by the Proviso in Part II of this Order;
 - iv. the identity or specific categories of such third parties; and
 - v. the purposes for sharing such covered information.
 2. 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.
- C. “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 Respondent 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 Respondent for preinstallation on a covered product by an operating system provider.
- D. “Clear(ly) and conspicuous(ly)” means that a required disclosure is difficult to miss (*i.e.*, easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
 1. 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.
 2. 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.
 3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
 4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

5. On a product label, the disclosure must be presented on the principal display panel.
 6. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.
 7. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
 8. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
 9. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, “ordinary consumers” includes reasonable members of that group.
- E. “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.
- F. “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 Respondent 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.

G. “Covered software” means:

1. Application software that injects advertisements into a consumer’s Internet browsing session, including pop-up advertisements; or
2. Application software that transmits, or causes to be transmitted, covered information to a person or entity other than the consumer, except when
 - a. 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
 - b. the covered information is transmitted or used solely for one or more of the following purposes:
 - i. being reasonably necessary for the software to perform a function or service that the consumer requests or otherwise interacts with;
 - ii. authenticating the consumer;
 - iii. configuring or setting up the software; or
 - iv. 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.

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. “Software provider” means any person or entity other than Respondent that sells, leases, licenses, or otherwise provides application software.

J. “Third party service provider” means any person or entity that is contractually required by Respondent or a software provider to: (a) use or receive covered information collected by or on behalf of Respondent or the software provider for and at the direction of Respondent or the 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 Respondent or the software provider; and (c) not use the covered information for any other purpose.

I. Prohibited Misleading Representations

IT IS ORDERED that Respondent, 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 Order, 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.

II. Affirmative Express Consent Provision

IT IS FURTHER ORDERED that, commencing no later than 120 days after the date of service of this Order, Respondent, 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 Order, whether acting directly or indirectly, shall not preinstall or cause to be preinstalled any covered software unless Respondent or the software provider:

- A. will obtain the consumer's affirmative express consent;
- B. provides instructions for how the consumer may revoke consent to the covered software's operation, which can include uninstalling the covered software; and
- C. 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.

III. Mandated Software Security Program

IT IS FURTHER ORDERED that Respondent must, no later than the date of service of this Order, 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 Respondent's size and complexity, the nature and scope of Respondent'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:

- A. the designation of an employee or employees to coordinate and be responsible for the software security program;
- B. 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;
- C. 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;
- D. the development and use of reasonable steps to select and retain software or service providers capable of maintaining security practices consistent with this Order, and requiring software and service providers, by contract, to implement and maintain appropriate safeguards; and
- E. the evaluation and adjustment of the software security program in light of the results of the testing and monitoring required by sub-provision C, any changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the software security program.

IV. Software Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with the Provision of this Order titled Mandated Software Security Program, Respondent must obtain initial and biennial assessments ("Assessments"):

- A. 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.

- B. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment, and (2) each 2-year period thereafter for 20 years after issuance of the Order for the biennial Assessments.
- C. Each Assessment must:
1. set forth the specific administrative, technical, and physical safeguards that Respondent has implemented and maintained during the reporting period;
 2. explain how such safeguards are appropriate to Respondent's size and complexity, the nature and scope of Respondent'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 Order 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.
- D. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Respondent must submit the initial Assessment to the Commission within 10 days after the Assessment has been completed. Respondent must retain all subsequent biennial Assessments, at least until the Order terminates. Respondent must submit any biennial Assessments to the Commission within 10 days of a request from a representative of the Commission.

V. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For 5 years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, and directors; (2) all employees, agents, and representatives with managerial responsibilities related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

VI. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondent makes timely submissions to the Commission:

- A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) identify all of Respondent's business entities by all of their names; (c) describe the activities of each business, including the goods and services offered; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the costs incurred and changes made by the Respondent to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.
- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (a) any designated point of contact; or (b) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
- C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within 14 days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____," and supplying the date, signatory's full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: *In re Lenovo (United States) Inc.*

VII. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for 20 years after the issuance date of the Order, and retain each such record for 5 years, unless otherwise specified below. Specifically, Respondent must create and retain the following records:

- A. accounting records showing the revenues from all covered products sold, the costs incurred in generating those revenues, and resulting net profit or loss;
- B. personnel records showing, for each person who must receive a copy of this Order pursuant to Part V.B., that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. copies or records of all U.S. consumer complaints relating to covered software or the security of application software, whether received directly or indirectly, such as through a third party, and any response;
- D. a copy of each representation subject to this Order;
- E. for 5 years after the date of preparation of each Assessment required by this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment; and
- F. all records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission.

VIII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

- A. Within 10 days of receipt of a written request from a representative of the Commission, Respondent must submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with any Respondent who has agreed to such an interview. The interviewee may have counsel present.

- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

IX. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate on December 20, 2037, or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. any Provision in this Order that terminates in less than 20 years;
- B. this Order's application to any Respondent that is not named as a defendant in such complaint; and
- C. this Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: December 20, 2017