142 3156

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of	**DECISION AND ORDER**
ASUSTeK Computer Inc., **a corporation.**	**DOCKET NO. C-4587**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named above 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) statements 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, and duly considered the comments filed thereafter by interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

1. Respondent ASUSTeK Computer, Inc., is a Taiwanese corporation with its principal office or place of business at 15, Li-Te Rd., Peitou, Taipei 11259, Taiwan.

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 shall apply:

1. Unless otherwise specified, "respondent" shall mean ASUSTeK Computer, Inc., corporation, and its subsidiaries and divisions in the United States, and successors and assigns.

2. "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:

   A. 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 is made in only one means.

   B. 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.

   C. 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.

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

   E. The disclosure must use diction and syntax understandable to ordinary consumers.

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

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

3. "Commerce" shall mean commerce among the several States or with foreign nations, or in any Territory of the United States or in the District of Columbia, or between any such Territory and another, or between any such Territory and any State or foreign nation, or between the District of Columbia and any State or Territory or foreign nation, as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

4. "Covered Device" shall mean (a) any router, or device for which the primary purpose is connecting other client devices to a network, developed by respondent, directly or indirectly, that is marketed to consumers in the United States and (b) the software used to access, operate, manage, or configure such router or other device subject to part (a) of this definition, including, but not limited to, the firmware, web or mobile applications, and any related online services, that are advertised, developed, branded, or provided by respondent, directly or indirectly, for use with, or as compatible with, the router or other device.

5. "Covered Information" shall mean any individually-identifiable information from or about an individual consumer collected by respondent through a Covered Device or input into, stored on, captured with, accessed, or transmitted through a Covered Device, including but not limited to (a) a first and last name; (b) a home or other physical address; (c) an email address or other online contact information; (d) a telephone number; (e) a Social Security number; (f) financial information; (g) an authentication credential, such as a username or password; (h) photo, video, or audio files; (i) the contents of any communication, the names of any websites sought, or the information entered into any website.

6. "Default Settings" shall mean any configuration option on a Covered Device that respondent preselects, presets, or prefills for the consumer.

7. "Software Update" shall mean any update designed to address a Security Flaw.

8. "Security Flaw" is a software vulnerability or design flaw in a Covered Device that creates a material risk of (a) unauthorized access to or modification of any Covered Device, (b) the unintentional exposure by a consumer of Covered Information, or (c) the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of Covered Information.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or indirectly, in or affecting commerce, must not misrepresent in any manner, expressly or by implication:

A. The extent to which respondent or its products or services maintain and protect:

1. The security of any Covered Device;

2. The security, privacy, confidentiality, or integrity of any Covered Information;

B. The extent to which a consumer can use a Covered Device to secure a network; and

C. The extent to which a Covered Device is using up-to-date software.

II.

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 security program that is reasonably designed to (1) address security risks related to the development and management of new and existing Covered Devices, and (2) protect the privacy, security, confidentiality, and integrity of Covered Information. Such program, the content and implementation of which must be fully documented in writing, must contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device's function or the Covered Information, including:

A. The designation of an employee or employees to coordinate and be accountable for the security program;

B. The identification of material internal and external risks to the security of Covered Devices that could result in unauthorized access to or unauthorized modification of a Covered Device, and assessment of the sufficiency of any safeguards in place to control these risks;

C. The identification of material internal and external risks to the privacy, security, confidentiality, and integrity of Covered Information that could result in the unintentional exposure of such information by consumers or 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;

D. At a minimum, the risk assessments required by Subparts B and C must include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including in secure engineering and defensive programming; (2) product design, development, and research; (3) secure software design, development, and testing, including for Default Settings; (4) review, assessment, and response to third-party security vulnerability reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures;

E. The design and implementation of reasonable safeguards to control the risks identified through risk assessment, including through reasonable and appropriate software security testing techniques, such as (1) vulnerability and penetration testing; (2) security architecture reviews; (3) code reviews; and (4) other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to Covered Devices and Covered Information is restricted consistent with a user's security settings;

F. Regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

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

H. The evaluation and adjustment of respondent's security program in light of the results of the testing and monitoring required by Subpart F, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of the security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent must obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments must be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience programming secure Internet-accessible consumer-grade devices; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and in programming secure Internet-accessible consumer-grade devices; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580. The reporting period for the Assessments must cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment must:

A. Set forth the specific controls and procedures that respondent has implemented and maintained during the reporting period;

B. Explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device's function or the Covered Information;

C. Explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and

D. Certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security of Covered Devices and the privacy, security, confidentiality, and integrity of Covered Information is protected and has so operated throughout the reporting period.

Each Assessment must be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent must provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments must be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin: *In re ASUSTek Computer Inc.*, FTC File No. 142 3156.

IV.

IT IS FURTHER ORDERED that respondent must:

A. Notify consumers, Clearly and Conspicuously, when a Software Update is available, or when respondent is aware of reasonable steps that a consumer could take to mitigate a Security Flaw. The notice must explain how to install the Software Update, or otherwise mitigate the Security Flaw, and the risks to the consumer's Covered Device or Covered Information if the consumer chooses not to install the available Software Update or take the recommended steps to mitigate the Security Flaw. Notice must be provided through at least each of the following means:

1. Posting of a Clear and Conspicuous notice on at least the primary, consumer-facing website of respondent and, to the extent feasible, on the user interface of any Covered Device that is affected;

2. Directly informing consumers who register, or who have registered, a Covered Device with respondent, by email, text message, push notification, or another similar method of providing notifications directly to consumers; and

3. Informing consumers who contact respondent to complain or inquire about any aspect of the Covered Device they have purchased.

B. Provide consumers with an opportunity to register an email address, phone number, device, or other information during the initial setup or configuration of a Covered Device, in order to receive the security notifications required by this Part. The consumer's registration of such information must not be dependent upon or defaulted to an agreement to receive non-security related notifications or any other communications, such as advertising. Notwithstanding this requirement, respondent may provide an option for consumers to opt-out of receiving such security-related notifications.

V.

IT IS FURTHER ORDERED that respondent must maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

A. For a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Part III of this order, for the compliance period covered by such Assessment;

B. Unless covered by V.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, all other documents relating to compliance with this order, including but not limited to:

1. All advertisements, promotional materials, installation and user guides, and packaging containing any representations covered by this order, as well as all materials used or relied upon in making or disseminating the representation;

2. All notifications required by Part IV of this order; and

3. Any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order.

VI.

IT IS FURTHER ORDERED that respondent must deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order. Respondent must deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such

position or responsibilities. For any business entity resulting from any change in structure set forth in Part VII, delivery must be at least ten (10) days prior to the change in structure.

VII.

IT IS FURTHER ORDERED that respondent must notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. *Provided, however*, that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent must notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin: *In re ASUSTek Computer Inc.*, FTC File No. 142 3156.

VIII.

IT IS FURTHER ORDERED that respondent, within sixty (60) days after the date of service of this order, must file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it must submit additional true and accurate written reports.

IX.

This order will terminate on July 18, 2036, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. Any Part in this order that terminates in fewer than twenty (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 Part.

Provided, further, that if such complaint is dismissed or a federal court rules that 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 as to such respondent will terminate according to this Part 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: July 18, 2016