0123240

UNITED STATES OF AMERICA
BEFORE FEDERAL TRADE COMMISSION

COMMISSIONERS: Timothy J. Muris, Chairman
Sheila F. Anthony
Mozelle W. Thompson
Orson Swindle
Thomas B. Leary

In the Matter of	)	**DOCKET NO. C-4069**
MICROSOFT CORPORATION, a corporation.	)	**DECISION AND ORDER**

The Federal Trade Commission having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 et seq; and

The respondent, its attorney, and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of said agreement is for settlement purposes only and does not constitute an admission by respondent that the law has been violated as alleged in such complaint, or that the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules.

The Commission having thereafter considered the matter and having determined that it has reason to believe that the respondent has violated the said Acts and Regulations, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days, and having duly considered the comments received, now in further conformity with the procedure described in § 2.34 of its Rules, the Commission hereby issues its complaint, makes the following jurisdictional findings and enters the following order:

1. Respondent Microsoft is a Washington corporation with its principal office or place of business at One Microsoft Way, Redmond, Washington 98052.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. "Personally identifiable information" or "personal information" shall mean individually identifiable information from or about an individual including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security Number; (f) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual; or (g) any information that is combined with any of (a) through (f) above.

2. "Covered online service" shall mean Passport, Kids Passport, Passport Wallet, any substantially similar product or service, or any multisite online authentication service.

3. Unless otherwise specified, "respondent" shall mean Microsoft Corporation, its successors and assigns and its officers, agents, representatives, and employees acting within the scope of their authority on behalf of, or in active concert or participation with Microsoft Corporation.

4. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of a covered online service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, its information practices, including:

A. what personal information is collected from or about consumers;

B. the extent to which respondent's product or service will maintain, protect or enhance the privacy, confidentiality, or security of any personally identifiable information collected from or about consumers;

C. the steps respondent will take with respect to personal information it has collected in the event that it changes the terms of the privacy policy in effect at the time the information was collected;

D. the extent to which the service allows parents to control what information their children can provide to participating sites or the use of that information by such sites; and

E. any other matter regarding the collection, use, or disclosure of personally identifiable information.

II.

IT IS FURTHER ORDERED that respondent, and its successors and assigns, in connection with the advertising, marketing, promotion, offering for sale, or sale of a covered online service, in or affecting commerce, shall establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program shall 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 personal information collected from or about consumers, including:

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

B. The identification of material internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, 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 should include consideration of risks in each area of relevant operation, including: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. Design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

D. Evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by paragraph C, 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 its information security program.

III.

IT IS FURTHER ORDERED that respondent obtain within one (1) year, and on a biannual basis thereafter, an assessment and report from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, that certifies:

A. that respondent has in place a security program that provides protections that meet or exceed the protections required by Part II of this order; and

B. that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumer's personal information has been protected.

The report required by this paragraph shall be prepared by a Certified Information System Security Professional (CISSP) or by a person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission.

IV.

IT IS FURTHER ORDERED that respondent, and its successors and assigns, shall for a period of five (5) years after the date of service of this order maintain and upon request make available to the Federal Trade Commission for inspection and copying a print or electronic copy of the following documents relating to compliance with this order:

A. a sample copy of each different print, broadcast, cable, or Internet advertisement, promotion, information collection form, Web page, screen, email message, or other document containing any representation to consumers regarding respondent's collection, use, and security of personal information from or about consumers. Each Web page copy shall be dated and contain the full URL of the Web page where the material was posted online. Electronic copies shall include all text and graphics files, audio scripts, and other computer files used in presenting the information on the Web. Provided, however, that after creation of any Web page

or screen in compliance with this order, respondent shall not be required to retain a print or electronic copy of any amended Web page or screen to the extent that the amendment does not affect respondent's compliance obligations under this order;

B. all plans, reports, studies, reviews, audits, audit trails, policies, and training materials, whether prepared by or on behalf of respondent, relating to respondent's compliance with this order; and

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

V.

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

VI.

IT IS FURTHER ORDERED that respondent Microsoft Corporation, and its successors and assigns, shall notify the Commission at least thirty (30) days prior to any change in the corporation 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 about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VII.

IT IS FURTHER ORDERED that respondent Microsoft Corporation, and its successors and assigns, shall within sixty (60) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which they have complied with this order.

VIII.

This order will terminate on December 20, 2022, or twenty (20) years from the most recent date that the United States or the Federal Trade 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 less 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 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 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: December 20, 2002