UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Division of Enforcement
Bureau of Consumer Protection

March 26, 2004

Charles E. Buffon, Esq.
Covington & Burling
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401

Re: Microsoft Corporation
Docket No. C-4069

Dear Mr. Buffon:

The Division of Enforcement staff has completed its review of the compliance report dated February 25, 2003, and of the supplemental submission dated May 23, 2003, filed by the respondent to show the manner and form of its compliance with the order referenced above issued on December 20, 2002. As you know, the staff also conducted an investigation involving the respondent's possible violations of the order.

The staff has determined that certain of the respondent's representations about covered online services are in violation of Part I of the order, which prohibits the respondent from misrepresenting its practices relating to the collection, use, or disclosure of personally identifiable information in connection with its marketing of covered online services. Accordingly, the staff is rejecting the following attachments to the respondent's February 25, 2003 compliance report:

CB 00019, CB 00032, CB 00116, and CB 00191. These exhibits represent that all .NET Passport-related cookies are deleted from users' computers when users sign out of .NET Passport. The respondent has indicated that .NET Passport users may have a cookie left on their computers to pre-fill their Passport usernames.

CB 00114. This exhibit represents that Microsoft Money 2002 files are unencrypted for users who do not also use .NET Passport. The respondent has indicated that Microsoft Money 2002 files are encrypted even if users do not also use .NET Passport. Thus, the exhibit incorrectly implies that the files are unencrypted if one uses Microsoft Money without Passport.

CB 00150. This exhibit, which is one webpage of a voluminous website, includes one statement that may lead parents to believe incorrectly that Kids Passport will allow them to select the type of personal information their children can share. The respondent has revised this exhibit to indicate clearly that Kids Passport only allows parents to control the sharing of information previously stored in a child's Passport profile.

CB 00126. This exhibit represents that .NET Passport never tracks user's online activity. The respondent has indicated that .NET Passport records a temporary log of individual sign-ins for system efficiency and security, and that this information is associated with personal information when a user calls customer service to request assistance.

The respondent, however, has advised the staff that it has either ceased disseminating the above representations or has modified them so that they are accurate.

As you are aware, as part of our compliance review, the staff investigated the circumstances surrounding a vulnerability in .NET Passport that was publicized in May of 2003. This vulnerability permitted a .NET Passport user to change the password on any other .NET Passport account. The order requires that the respondent implement and maintain a reasonable and appropriate security program. Accordingly, our concern was whether the existence of this vulnerability reflected a failure to implement appropriate security measures as required by the order. During the course of the investigation, the staff found the following:

- The vulnerability was created during a software revision that occurred prior to the date the order went into effect and resulted from problems in coding documentation and change control.

- As part of its compliance with Part II of the order, Microsoft has implemented several changes to its software revision process to prevent the creation of security vulnerabilities, including requiring annotations for software code that enhances security and requiring security reviews of code changes. These revised processes are likely to prevent the introduction of further vulnerabilities similar to the password-reset vulnerability during software revisions.

- As part of its security program, and pursuant to the order, Microsoft monitors potential threats to the Passport system and adjusts its security measures accordingly. At the time the password-reset vulnerability was publicized, Microsoft had already identified other similar potential vulnerabilities and was in the process of implementing security measures to address those potential vulnerabilities. These measures would have eliminated the password-reset vulnerability even if it had never been publicized.

The staff's extensive review of Microsoft's compliance with the order did not find evidence that the company failed to implement and maintain a reasonable information security program as required by Part II of the order. Furthermore, because the order was not in effect when the password-reset vulnerability was created, the staff has concluded that the existence of the password-reset vulnerability did not constitute or prove an order violation.

The staff has concluded, on the assumption that the information submitted is accurate and complete, that no compliance action is indicated at this time, and the investigation has been closed. We will not be precluded, however, from recommending to the Commission an appropriate action if the submitted information is inaccurate or incomplete or if the respondent violates the terms of the order. Please be advised that the opinions expressed in this letter are those of the staff and not necessarily those of the Commission or of any Commissioner. You will be advised of the General Counsel's determinations concerning the respondent's request for confidential treatment of certain documents by separate letter.

Sincerely,

Elaine D. Kolish
Associate Director