Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Oracle Corporation, File No. 132 3115

The Federal Trade Commission has accepted, subject to final approval, an agreement containing a consent order applicable to Oracle Corporation ("Oracle").

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

Oracle is a Delaware corporation that, among other things, develops the Java computing platform, which is used to power applications that, for example, allow consumers to play online games, chat with people online, calculate mortgage interest, and view images in 3D. Consumers primarily use the Java Platform, Standard Edition ("Java SE"). When an update to Java SE was available, a consumer would typically receive a prompt to update the software. When the consumer proceeded to install the update, the consumer would encounter a series of installation screens, which stated that "Java provides safe and secure access to the world of amazing Java content," and that Java SE updates and a consumer's "system" would have "the latest . . . security improvements." During the Java SE update process, however, Oracle did not inform consumers that Java SE updates automatically removed only the most recent prior iteration of Java SE installed on the consumer's computer, even if the consumer had multiple iterations of Java SE installed, and that the update would not remove any iteration released prior to Java SE iteration 6 update 10. As such, after the update process, consumers could still have additional older, insecure iterations of Java SE installed on their computers, which attackers targeted to obtain consumers' personal information through malware designed to exploit vulnerabilities ("exploit kits").

The Commission's complaint alleges that Oracle violated Section 5(a) of the FTC Act by failing to disclose that, in numerous instances, updating Java SE would not delete or replace all older iterations of Java SE on a consumer's computer, and as a result, a consumer's computer could still have iterations of Java SE installed that are vulnerable to security risks. This fact would be material to consumers' decisions whether to take further action after "updating" Java SE to protect their computers, in light of Oracle's representations to consumers that by updating Java SE, users would ensure that Java SE on their computers had the latest security improvements.

The complaint further alleges that, by failing to inform consumers that the Java SE update process did not remove all prior iterations of the software, Oracle left some consumers vulnerable to a serious, well-known, and reasonably foreseeable security risk that attackers would target these computers through exploit kits, resulting in the theft of personal information. Consumers with insecure iterations of Java SE on their computers were vulnerable to exploit kits targeting Java SE vulnerabilities while browsing infected websites or clicking on nefarious links. Attackers used exploit kits targeting Java SE vulnerabilities to install key loggers that captured consumers' usernames and passwords, which could be used to log into a consumer's PayPal, bank, and credit card accounts. Other Java SE exploit kits may

have resulted in the unauthorized acquisition and transmission of sensitive personal information for the purpose of targeted spear-phishing campaigns.

The proposed order contains provisions designed to prevent Oracle from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits Oracle from misrepresenting (1) the privacy or security of the covered software on a consumer's computer, including but not limited to the effect on privacy or security of any installation or update of the covered software; and (2) how to uninstall older iterations of the covered software.

Part II of the proposed order requires Oracle to ensure that during any installation or update of any iteration of Java SE released after the date of service of the order, Oracle:

(1) clearly and conspicuously discloses to the consumer all iterations of Java SE 1.4.2 or later, other than any iteration(s) released within the last quarter, currently installed on the consumer's computer;

(2) clearly and conspicuously explains that there may be risks to the security of the consumer's computer if the consumer chooses not to remove any iterations of Java SE older than the iteration(s) released within the last quarter currently installed on the consumer's computer; and

(3) clearly and conspicuously discloses which iterations of Java SE 1.4.2 or later, other than any iteration(s) released within the last quarter, that remain installed following installation or update of Java SE, and clearly and conspicuously provides instructions describing how consumers can effectively uninstall these iterations.

Part III of the proposed order requires Oracle to notify consumers who downloaded, installed, or updated Java SE that, in some instances, they may have older, insecure iterations of Java SE on their computers; and provide instructions to such consumers on how to remove these older iterations. In addition, for three (3) years, Oracle must provide an uninstall tool that allows consumers to uninstall iterations of Java SE 1.4.2 or later; a page on their primary website that explains how to uninstall older, insecure iterations of Java SE; and free support through an electronic form to help consumers with their update and/or uninstall issues.

Parts IV through VIII of the proposed order are standard reporting and compliance provisions. Part IV requires Oracle to retain documents relating to its compliance with the order for a five-year period. Part V requires dissemination of the order now and in the future to all current and future principals, officers, directors, and managers, and to persons with managerial or supervisory responsibilities relating to Parts I – III of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates that Oracle submit a compliance report to the FTC within 90 days, and periodically thereafter as requested. Part VIII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed complaint or order or to modify the order's terms in any way.