132 3115

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

In the Matter of	)	**DOCKET NO. C-4571**
ORACLE CORPORATION, a corporation.	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that Oracle Corporation has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Oracle Corporation ("Oracle") is a Delaware corporation with its principal office or place of business at 500 Oracle Parkway, Redwood City, California 94065.

2. The acts and practices of Oracle as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

ORACLE'S BUSINESS PRACTICES

3. Oracle is a software company that, among other things, develops the Java computing platform ("Java"), which is used to power many types of applications. Some of the more common Java applications allow consumers to play online games, chat with people online, calculate mortgage interest, and view images in 3D. Oracle acquired Java on January 27, 2010, as part of its purchase of Sun Microsystems, Inc.

4. Java comes in multiple editions for both enterprises and consumers. Consumers primarily use the Java Platform, Standard Edition ("Java SE"), which has been installed on more than 850 million personal computers.

5. Java SE includes various components that enable consumers to run Java applications on websites. Many computers today are sold with Java SE pre-installed. Alternatively, a consumer may go to the Java.com website and download Java SE.

JAVA SE SECURITY

6. Since at least 2010, a principal security challenge facing Java SE users was that attackers closely monitored Oracle's release of updates to its software to identify vulnerabilities in Java SE's previous iterations. At the same time, attackers often developed malware designed to exploit vulnerabilities in previous iterations of Java SE installed on users' computers ("exploit kits").

7. In late 2010, Oracle acknowledged that exploit kits for at least 44 Java SE vulnerabilities were publicly available. For example, attackers have used known exploit kits targeting Java SE vulnerabilities to install key loggers that would capture consumers' usernames and passwords, which could be used to log into a consumer's PayPal, bank, and credit card accounts.

8. Other Java exploit kits could result in the unauthorized acquisition and transmission of sensitive personal information for the purpose of targeted spear-phishing campaigns.

9. 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.

THE JAVA SE UPDATE PROCESS

10. Oracle released Java SE version 6 update 19 in March 2010. Oracle released several subsequent updates for Java SE version 6 through April 16, 2013.

11. When an update was available, consumers would typically receive a prompt to update their Java SE. 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" (*see, e.g.*, Exhibit B) would have "the latest . . . security improvements." (*See, e.g.*, Exhibits A–B).

12. In its 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. Updates would also not remove any iteration released prior to Java SE version 6 update 10. Therefore, after the update process, consumers could still have additional older, insecure iterations of Java SE on their computers.

13. Beginning in October 2010, in a separate FAQ page of Oracle's website, Oracle explained that because, in the past, consumers would install "each Java update . . . in separate directories on [their] system," consumers "may have installed multiple versions of Java." (*See, e.g.*, Exhibits C–D). In addition, Oracle explained to consumers that additional "old and unsupported versions of Java on your system present[] a serious security risk" and that "[r]emoving older versions of Java from your system ensures that

Java applications will run with the most up-to-date security." (*See, e.g.*, Exhibits C–D). However, for any consumers sophisticated enough to find this page on their own, it did not inform them that the Java SE update process did not automatically remove all older, insecure iterations of the software. In addition, Oracle failed to disclose this information or link to the relevant FAQ page during the Java SE update process.

14. Oracle was aware, no later than 2011, that its Java SE update process was not sufficient to ensure that consumers could always remove older, insecure iterations of Java SE and, therefore, that Java SE on their systems would have the latest security improvements. In internal documentation, Oracle admitted that "Java malware propagation [was] successful even though [attackers are] exploiting fixed bugs" and that the "Java update mechanism is not aggressive enough or simply not working." Nevertheless, Oracle did not inform consumers during the update process that updating Java SE did not remove all older iterations of Java SE on their computers, and therefore, that their computers could remain susceptible to exploit kits targeting Java SE vulnerabilities.

15. In July 2011, Oracle released Java SE version 7. Oracle then began to periodically release updates for Java SE version 7. In December 2012, Oracle began to prompt certain users to update from Java SE version 6 to Java SE version 7. These updates continued to remove only the most recent prior iteration of Java SE.

16. In March 2014, Oracle released Java SE version 8. Oracle then began to periodically release updates for Java SE version 8. These updates continued to remove only the most recent prior iteration of Java SE until August 2014.

IMPACT ON CONSUMERS

17. In numerous instances, Java SE's update and uninstallation issues made it likely that consumers unknowingly would have older, insecure iterations of Java SE installed.

18. Attackers used exploit kits to specifically target vulnerabilities in older, insecure iterations of Java SE installed on consumers' computers. As described in Paragraph 7, attackers used these exploit kits to obtain consumers' personal information.

19. 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, as described above.

VIOLATION OF THE FTC ACT

Failure to Disclose

20. As described in Paragraph 11, Oracle represented, directly or indirectly, expressly or by implication, that by updating Java SE, Java users would ensure that Java SE on their computers had the latest security improvements.

21. Oracle failed to disclose, or failed to disclose adequately, 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' decision whether to take further action after "updating" Java SE to protect their computers.

22. Oracle's failure to disclose, or disclose adequately, the material information described in Paragraph 21, in light of the representation set forth in Paragraph 20, is a deceptive act or practice.

23. The acts and practices of Oracle as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this twenty-eighth day of March, 2016, has issued this complaint against Oracle.

By the Commission.

Donald S. Clark
Secretary

SEAL: