102-3076

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Jon Leibowitz, Chairman**
William E. Kovacic
J. Thomas Rosch
Edith Ramirez
Julie Brill

In the Matter of	)	
LOOKOUT SERVICES, INC.,	)	
a corporation.	)	**DOCKET NO. C- 4326**

The Federal Trade Commission, having reason to believe that Lookout Services, Inc. ("respondent" or "Lookout") 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 Lookout is a Texas corporation, with its principal office or place of business at 5909 West Loop South, Suite 300, Bellaire, Texas 77401.

2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

3. At all relevant times, Lookout has been in the business of selling a web-based computer product known as the I-9 Solution. This product is designed to help employers comply with their obligations under federal law to complete and maintain a U.S. Citizenship and Immigration Services Form I-9 about each employee in order to verify that the employee is eligible to work in the United States.

4. The I-9 Solution routinely collects and stores information from or about its customers' employees, including, but not limited to, names; addresses; dates of birth; Social Security numbers; passport numbers; alien registration numbers; driver's license numbers; and military identification numbers. This highly sensitive information is maintained in Lookout's database (the "I-9 database"). The misuse of such information – particularly Social Security numbers – can facilitate identity theft and related consumer harms.

5. Since at least April 2009, Lookout has disseminated or caused to be disseminated statements in its marketing materials, including, but not limited to, the following statement regarding the security of data it maintains:

> *Secure Your Data*
> Although the data is entered via the web, your data will be encoded and transmitted over secured lines to Lookout Services server. This FTP interface will protect your data from interception, as well as, keep the data secure from unauthorized access.

6. Since at least 2006, Lookout's website has made the following claim:

> Perimeter Defense – Our servers are continuously monitoring attempted network attacks on a 24 x 7 basis, using sophisticated software tools.

7. Since at least 2006 and continuing through at least the Fall of 2009, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on Lookout's networks. Among other things, respondent:

   a. failed to implement reasonable policies and procedures for the security of sensitive consumer information collected and maintained by Lookout;

   b. failed to establish or enforce rules sufficient to make user credentials (i.e., user ID and password) hard to guess. For example, respondent did not require its customers or employees to use complex passwords to access the I-9 database. Accordingly, users could select the same word, including common dictionary words, as both the password and user ID, or a close variant of the user ID as the password;

   c. failed to require periodic changes of user credentials, such as every 90 days, for customers and employees with access to sensitive personal information;

   d. failed to suspend user credentials after a certain number of unsuccessful login attempts;

   e. did not adequately assess and address the vulnerability of Lookout's web application to widely-known security flaws, such as "predictable resource location," which enables users to easily predict patterns and manipulate the uniform resource locators ("URLs") to gain access to secure web pages;

   f. allowed users to bypass the authentication procedures on Lookout's website when they typed in a specific URL;

g. failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as by employing an intrusion detection system and monitoring system logs; and

h. created an unnecessary risk to personal information by storing passwords used to access the I-9 database in clear text.

8. In October 2009, and again in December 2009, Lookout's weak authentication practices and web application vulnerabilities enabled an employee of a Lookout customer to gain access to the personal information of over 37,000 consumers.

9. Specifically, in October 2009, the employee obtained a URL for a secure web page during a webinar for the I-9 Solution. She later typed that URL into her browser and gained access to a portion of the I-9 database. By typing the precise URL into the browser, she bypassed the Lookout login page, and was never prompted to provide a valid user credential. The employee then made minimal and easy-to-guess changes to the URL and gained access to the entire I-9 database.

10. In December 2009, the employee visited Lookout's public-facing login web page for the I-9 Solution where she guessed and entered several different user IDs and passwords, including the user ID "test" and the password "test." Because this was a valid user credential for one of Lookout's customers, entering "test" and "test" gave her access to the personal information of the more than 11,000 consumers employed by that customer. Then, by making minimal and easy-to-guess changes to the URL, the employee again gained access to the entire I-9 database, which included the personal information of more than 37,000 consumers.

11. Because Lookout did not employ an intrusion detection system until October 2009, or adequately monitor system logs until December 2009, it is unknown if other unauthorized persons accessed the personal information in the I-9 database before that time.

12. Following the October and December 2009 breaches, Lookout took steps to prevent additional unauthorized access to the I-9 database, including disabling the "test" account and instituting certain code patches to its application. In January 2010, Lookout mailed breach notification letters to customers whose accounts the employee may have viewed.

VIOLATIONS OF THE FTC ACT

13. Through the means described in Paragraphs 5 and 6, respondent represented, expressly or by implication, that it implemented reasonable and appropriate measures to protect personal information against unauthorized access.

14. In truth and in fact, as described in Paragraph 7, respondent did not implement