Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Lookout Services, Inc., File No. 1023076

The Federal Trade Commission has accepted, subject to final approval, a consent order applicable to Lookout Services, Inc.

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.

The Commission's complaint alleges that Lookout sells 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. The complaint alleges that the I-9 Solution routinely collects and stores information about Lookout's c

locators ("URL") 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.

Each of these failures could have been remedied using well-known, readily available, and/or free or low-cost data security measures.

The complaint further alleges that, as a result of these failures, an employee of a Lookout customer was able to obtain unauthorized access to Lookout's I-9 database on two separate occasions between October and December 2009. In both instances, the employee gained unauthorized access to the personal information, including Social Security numbers, of more than 37,000 consumers. Given the sensitive nature of the personal information exposed, the company's failure to provide reasonable and appropriate security for this information is likely to cause consumers substantial injury as described above. That substantial injury is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. The complaint alleges that Lookout's failure to employ reasonable and appropriate measures to prevent unauthorized access to sensitive personal information is an unfair act or practice and that the company misrepresented that it had implemented such measures, in violation of Section 5 of the Federal Trade Commission Act.

The proposed order applies to personal information that Lookout collects from or about consumers and employees. It contains provisions designed to prevent Lookout from engaging in the future in practices similar to those alleged in the complaint.

Part I of t

of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks;

- design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly