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 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, which do not expire – can facilitate identity theft, including existing and new account fraud, and related consumer harms.

The complaint alleges that, since at least 2006, Lookout engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for the personal information it collected and maintained. The challenged practices are fundamental security failures, most of which have been challenged in prior FTC data security cases. Among other things, Lookout:

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

b. failed to establish or enforce rules sufficient to make user credentials (*i.e.*, user ID and password) hard to guess;

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 its 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 ("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 the proposed order prohibits misrepresentations about the privacy, confidentiality, or integrity of personal information collected from or about consumers. Part II of the proposed order requires Lookout to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to Lookout's size and complexity, the nature and scope of its activities, and the sensitivity of the information collected from or about consumers and employees. Specifically, the proposed order requires Lookout to:

- designate an employee or employees to coordinate and be accountable for the information security program;

- identify material internal and external risks to the security, confidentiality, and integrity

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 test or monitor the effectiveness of the safeguards' key controls, systems, and procedures;

- develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from Lookout, and require service providers by contract to implement and maintain appropriate safeguards; and

- evaluate and adjust its information security programs in light of the results of testing and monitoring, any material changes to operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on its information security program.

Part III of the proposed order requires Lookout to obtain within the first one hundred eighty (180) days after service of the order, and on a biennial basis thereafter for a period of twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) it has in place a security program that provides protections that meet or exceed the protections required by Part II of the proposed order; and (2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of sensitive consumer, employee, and job applicant information has been protected.

Parts IV through VIII of the proposed order are reporting and compliance provisions. Part IV requires Lookout to retain documents relating to its compliance with the order. For most records, the order requires that the documents be retained for a five-year period. For the third-party assessments and supporting documents, Lookout must retain the documents for a period of three years after the date that each assessment is prepared. Part V requires dissemination of the order now and in the future to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates that Lookout submit a compliance report to the FTC within 60 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 order or to modify its terms in any way.