Analysis of the Proposed Consent Order to Aid Public Comment
In the Matter of Compete, Inc., File No. 102 3155

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

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.

Compete develops software for tracking consumers as they shop, browse and interact with different websites across the Internet. As alleged in the Commission's complaint, Compete offered one version of its tracking software as the Compete Toolbar, which would provide consumers with information about websites as they surfed the web, such as information about the popularity of the websites they visited. Separately, Compete offered consumers membership in its Consumer Input Panel: consumers could win rewards while participating in surveys about products and services. As part of the registration process for the Consumer Input Panel, consumers would install tracking software. In addition, Compete licensed its tracking software to third parties, such as Upromise, Inc., which was the subject of a recent FTC enforcement action. (See Upromise, Inc.)<hyperlink to Upromise case http://www.ftc.gov/os/caselist/1023116/index.shtm>

The Commission's complaint involves the advertising, marketing and operation of tracking software. According to the FTC complaint, while Compete represented to consumers that the various forms of software would collect information about the web sites consumers visited, its failure to disclose the full extent of data collected through tracking software was deceptive. The complaint alleges that Compete's tracking software collected the names of all websites visited; all links followed; advertisements displayed when websites were visited; and information that consumers entered into some web pages (e.g., credit card and financial account numbers, usernames, passwords, and search terms), including secure web pages.

According to the FTC complaint, Compete misrepresented its privacy and security practices, including that: 1) it stripped all personal information out of the data it collected before transmitting it from consumers' computers; and 2) it employed reasonable and appropriate measures to protect data gathered from consumers from unauthorized access. The complaint alleges that these claims were false and thus violate Section 5 of the FTC Act.

In addition, the FTC complaint alleges that Compete 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 complaint alleges that, among other things, Compete: 1) transmitted sensitive information from secure web pages, such as financial account numbers and security codes, in clear readable text; 2) did not design and implement reasonable safeguards to control risks to consumer information; and 3) did not use readily available, low-cost measures to

assess and address the risk that its software would collect sensitive consumer information it was not authorized to collect.

The complaint alleges that Compete's failure to employ reasonable and appropriate measures to protect consumer information – including credit card and financial account numbers, security codes and expiration dates, and Social Security numbers – was unfair. Tools for capturing data in transit, for example over unsecured wireless networks such as those often provided in coffee shops and other public spaces, are commonly available, making such clear-text data vulnerable to interception. The misuse of such information – particularly financial account information and Social Security numbers – can facilitate identity theft and related consumer harms.

The complaint alleges that after flaws in Compete's data collection practices were revealed publicly in January 2010, Compete upgraded its filters, added new algorithms to screen out information such as credit card numbers, and began encrypting data in transit.

The proposed order contains provisions designed to prevent Compete from engaging in future practices similar to those alleged in the complaint. For purposes of the proposed consent order, we call such tracking software a "Data Collection Agent."[1]

Part I applies to collection and use of data from any Data Collection Agent, whether already downloaded or to be downloaded in the future, and is tailored to address distribution by both Compete and third parties. Specifically Parts I.A. and B. of the proposed order apply to Data Collection Agents installed after the date of service of the order. Part I.A. prohibits Compete from collecting data through a Data Collection Agent unless a consumer has given express affirmative consent to such collection, after being provided with a separate, clear and prominent notice about all the types of information that will be collected, as well as a description of how the information is to be used, including any sharing with third parties. Part I.B. ensures these same protections apply when a Data Collection Agent is made available by a third party, and requires that Compete must either provide notice and obtain consent, or require the third party to do so and monitor the third party's compliance. In addition, Parts I.C. and D. of the proposed order limit the collection and use of data from consumers who already have downloaded a Data Collection Agent (i.e., before the date of service of the order) to aggregate and anonymous data, absent notice and affirmative express consent. Part I.E. requires Compete to obtain express affirmative consent before it can make any material changes to its practices for collection or sharing of personal information.

---

[1] "Data Collection Agent" is defined in the proposed order as any software program, including any application; created, licensed or distributed, directly or through a Third Party, by respondent; installed on consumers' computers, whether as a standalone product or as a feature of another product; and used to record, or transmit information about any activity occurring on that computer, unless: (a) the activity involves transmission of information related to the configuration of the software program or application itself; (b) the transmission is limited to information about whether the program is functioning as intended; or (c) the activity involves a consumer's interactions with respondent's websites and/or forms.

Part II.A. of the proposed order requires Compete to provide corrective notice to consumers who had previously installed a Data Collection Agent. Compete must inform consumers about the categories of personal information collected and transmitted by the software, and how to uninstall it. Part II.B. requires the company to provide for two years phone and e-mail support to assist consumers who seek to disable or uninstall a Data Collection Agent.

Part III of the proposed order requires Compete to provide a copy of the order to third parties with whom it has now, or will have in the future, any agreement in connection with any Data Collection Agent made available by the third party.

Part IV of the proposed order prohibits the company from making any misrepresentations about the extent to which it maintains and protects the security, privacy, confidentiality, or integrity of any information collected from or about consumers.

Part V of the proposed order requires Compete to maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of information (whether in paper or electronic format) about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to Compete's size and complexity, the nature and scope of its activities, and the sensitivity of the information. Specifically, the proposed order requires Compete 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 Compete or obtain on behalf of Compete, 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 VI of the proposed order requires Compete to obtain within 180 days after service of the order, and biennially thereafter for 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 the proposed order; and 2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Part VII requires Compete to destroy all consumer data collected by a Data Collection Agent before February 2010.

Part VIII requires Compete to retain documents relating to its compliance with the order. Part IX requires that it deliver copies of the order to persons with responsibilities relating to the subject matter of the order. Parts X, XI, and XII of the proposed order are further reporting and compliance provisions. Part X ensures notification to the FTC of changes in corporate status. Part XI mandates that Compete submit a compliance report to the FTC within 60 days, and periodically thereafter as requested. Part XII provides that the order will terminate after 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 proposed order's terms in any way.