Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Upromise, Inc., File No. 102 3116

The Federal Trade Commission has accepted, subject to final approval, an agreement containing a consent order applicable to Upromise, 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.

Upromise offers, among other things, a membership service through which consumers who join can receive cash rebates for making online purchases from merchants who participate in the Upromise program. To take part in the program, consumers download and install software, the Upromise TurboSaver Toolbar ("Toolbar"), from Upromise that modifies the consumers' Internet browser to highlight Upromise member merchants.

The Commission's complaint involves the advertising, marketing, and operation of an optional feature of that Toolbar, the "personalized offers" feature. That feature modified the Toolbar to provide targeted advertising to the consumer based upon the consumers' online behavior (the modified version is referred to here as the "Targeting Tool"). Upromise engaged a service provider to develop the Toolbar and the personalized offers feature.

According to the FTC complaint, while Upromise represented to consumers that the Targeting Tool collected information about the web sites consumers visited, its failure to disclose the full extent of data collected through the software was deceptive. The complaint alleges that the Targeting Tool collected the names of all websites visited; all links clicked; information that consumers entered into some web pages such as usernames, passwords, and search terms; and, from July 2009 through mid-January 2010, consumers' interactions with forms on secure web pages. The complaint further alleges that Upromise misrepresented its privacy and security practices, including misrepresenting that consumers' data would be encrypted. The complaint alleges that these claims were false and thus violate Section 5 of the FTC Act.

In addition, the FTC complaint alleges that Upromise engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for the personal information it collected and maintained. Among other things, Upromise: (1) transmitted sensitive information from secure web pages, such as financial account numbers and security codes, in clear readable text; (2) did not use readily available, low-cost measures to assess and address the risks to consumer information; (3) failed to ensure that employees responsible for the information collection program received adequate guidance and training; (4) failed to take adequate measures to ensure that its service provider employed reasonable and appropriate measures to protect consumer information.

The complaint alleges that Upromise'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 proposed order contains provisions designed to prevent Upromise from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order requires Upromise to disclose to consumers – before the download or installation of software that records or transmits information about any activity occurring on a computer involving the computer's interactions with websites, services, applications, or forms – the types of information collected and how the information will be used. The disclosure must be clear and prominent and separate from other notices. The company must also obtain consumers' express affirmative consent before the consumer downloads, installs, or otherwise activates such software. In addition, the company must provide this clear and prominent notice, and obtain express affirmative consent, before enabling data collection through any previously installed TurboSaver Toolbar and before making any material change from stated practices about collection or sharing of personal information through the Toolbar.

Part II of the proposed order requires Upromise to provide notice to consumers who, prior to the issuance of the order, had the Personalized Offers feature enabled. The notice must inform consumers about the categories of personal information that were, or could have been, transmitted by the feature, and how to disable the Personalized Offers feature and uninstall the Toolbar. Part III of the proposed order requires the company to destroy data it collected during the years covered by the complaint unless otherwise directed by the Commission.

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 complaint requires Upromise to maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of such information (whether in paper or electronic format) about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to Upromise'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 Upromise 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 Upromise or obtain on behalf of Upromise, 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 Upromise 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 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 VII, VIII, IX, X, XI, and XII of the proposed order are reporting and compliance provisions. Part VII requires Upromise 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, Upromise must retain the documents for a period of three years after the date that each assessment is prepared. Part VIII requires the company to cooperate with the FTC in connection with this action or any subsequent investigations related to or associated with the transactions or the occurrences that are the subject of the FTC complaint. Part IX requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part X ensures notification to the FTC of changes in corporate status. Part XI mandates that Upromise submit a compliance report to the FTC within 60 days, and periodically thereafter as requested. Part XII provides that the order will terminate 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.