102 3116

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

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

In the Matter of	)	
UPROMISE, INC.,	)	
a corporation.	)	
	)	**DOCKET NO. C-4351**

COMPLAINT

The Federal Trade Commission, having reason to believe that Upromise, Inc. ("Upromise" or "respondent"), a corporation, has violated the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Upromise is a Delaware corporation with its principal office at 95 Wells Avenue, Suite 160, Newton, Massachusetts 02459.

2. The acts and practices of respondent, as alleged herein, have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act.

RESPONDENT'S BUSINESS PRACTICES AND REPRESENTATIONS TO CONSUMERS

3. Upromise offers a membership service to consumers. A consumer who is a member of Upromise and purchases products and services from Upromise partner merchants can receive cash rebates. Upromise places these cash rebates into a college savings account for the consumer.

4. Since 2005, Upromise disseminated or caused to be disseminated through its website, www.upromise.com, a software toolbar referred to as the Upromise TurboSaver Toolbar (the "Toolbar") for consumers to download and install onto their computers. Among other things, the Toolbar highlighted Upromise partner companies in consumers' search results, so that consumers could more easily determine which companies were Upromise partners. (*See* Exhibit 1).

5. The Toolbar incorporated a "personalized offers" feature that, when enabled, would collect and transmit information through the consumer's browser. The personalized offers feature used consumer browsing information to provide targeted advertising to consumers through the browser. Upromise engaged a service provider to develop the Toolbar and the personalized offers feature.

6. During the download process for the Toolbar, where the personalized offers feature was offered users were presented with one of several versions of a pop-up window that contained a check-box next to text stating "Enable Personalized Offers," (*See, e.g.*, Exhibits 2- 4). Until mid-January 2010, Upromise provided the following description of the personalized offers feature, either directly in the pop-up window or if the consumer clicked on a hyperlink labeled "Show":

> By enabling the Personalized Offers feature, information about the web sites you visit will be collected. This information is used to provide college savings opportunities tailored to you.
>
> *See, e.g.*, Exhibit 2, Exhibit 3 (operational from approximately July 2009 to January 2010), and Exhibit 4 (operational from approximately October 2008 to May 2009).

In some instances, the check-box to "Enable Personalized Offers" was pre-checked to enable the personalized offers feature by default. (*See, e.g.*, Exhibit 2, operational from approximately July 2009 to January 2010).

7. When the personalized offers feature was enabled, the feature modified the Toolbar to collect extensive information about consumers' online activities and transmit it to the service provider for analysis. (Hereafter this modified version of the Toolbar with the personalized offers feature enabled is referred to as the "Targeting Tool.") The Targeting Tool collected the names of all websites visited, all links clicked, and information that consumers entered into some web pages such as usernames, passwords, and search terms. The Targeting Tool's data collection occurred in the background as a consumer used the Internet, and there was no way for consumers – without special software and technical expertise – to discover the extent of the data collection. Moreover, from July 2009 to mid-January 2010, the Targeting Tool was reconfigured to include consumers'

interactions with forms on secure web pages, which companies such as banks and online retailers provide to safeguard consumer data. The Targeting Tool was enabled on at least 150,000 consumers' computers.

8. The Upromise TurboSaver™ Privacy Statement, which was available on the Upromise website and at times through a link during the download process, stated that the Toolbar might "infrequently" collect some personal information. It further stated that a filter, termed a "proprietary rules engine," would "remove any personally identifiable information" prior to transmission. (*See, e.g.,* Exhibit 5, operational from approximately October 2008 to September 2009). The TurboSaver™ Privacy Statement also stated that "every commercially viable effort" would be made "to purge their databases of any personally identifiable information."

9. In fact, although a filter was used to instruct the Targeting Tool to avoid certain data, the filter was too narrow and improperly structured. For example, although the filter was intended to prevent the collection of financial account personal identification numbers and would have prevented collection of that data if a website used the field name "PIN," the filter would not have prevented such collection if a website used field names such as "personal ID" or "security code."

10. The Targeting Tool transmitted the information it gathered – including in some cases credit card and financial account numbers, security codes and expiration dates, and Social Security numbers entered into web pages, including secure web pages – over the Internet in clear text. 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.

11. On approximately January 21, 2010, Upromise halted all data collection through the Targeting Tool after a security researcher disclosed the scope of the information collected and the fact that it was transmitted in clear text.

12. In addition to the representations made in the download process and in the Upromise TurboSaver™ Privacy Statement, respondent has disseminated or caused to be disseminated the Upromise Privacy Statement, which was available on the Upromise website and through a link in the TurboSaver™ Privacy Statement. The Upromise Privacy Statement stated:

> Upromise is committed to earning and keeping your trust. We understand the need for our customers' personal information to remain secure and private and we have implemented policies and procedures designed to safeguard your information.
>
> Exhibit 6 (operational from approximately June 2008 to January 2010).

13. Similarly, the Upromise Security Statement, also available on the Upromise website, stated:

> Our members' security and privacy are critically important issues for Upromise. We are proud of the innovations we have made to protect your data and personal identity throughout the Upromise service. Upromise protects your data by... SSL, Data, and Password encryption technology....
>
> Using the Secure Sockets Layer protocol (SSL), Upromise automatically encrypts your sensitive information in transit from your computer to ours.
>
> * * *
>
> Upromise security architecture and security procedures are audited and inspected by industry leaders specializing in security processes and technologies.
>
> Exhibit 7 (operational from approximately January 2008 to January 2010).

14. Respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for consumer information collected and transmitted by the Targeting Tool. Among other things, respondent:

    a. created unnecessary risks of unauthorized access to consumer information by the Targeting Tool transmitting sensitive information from secure web pages, such as financial account numbers and security codes, in clear readable text over the Internet;

    b. failed to use readily available, low-cost measures to assess and address the risk that the Targeting Tool would collect such sensitive consumer information it was not authorized to collect. For example, respondent did not test the Targeting Tool before distributing it to consumers or monitor the Targeting Tool's operation thereafter to verify that the information it collected was consistent with respondent's policies;

c. failed to ensure that employees responsible for the information collection program received adequate guidance and training about security risks and respondent's privacy and security policies; and

d. failed to take adequate measures to ensure that its service provider employed reasonable and appropriate measures to protect consumer information and to implement the information collection program in a manner consistent with the respondent's privacy and security policies and contractual provisions designed to protect consumer information.

VIOLATIONS OF THE FTC ACT

Count 1

15. Through the means described in Paragraph 6, respondent has represented, expressly or by implication, that the Targeting Tool would collect and transmit information about the websites consumers visit. Respondent failed to disclose that the Targeting Tool would also collect and transmit much more extensive information about the Internet behavior that occurs on consumers' computers, and, for the period between July 2009 and January 2010, information consumers provided in secure sessions when interacting with third-party websites, shopping carts, and online accounts – such as credit card and financial account numbers, security codes and expiration dates, and Social Security numbers consumers entered into such web pages. These facts would be material to consumers. Respondent's failure to disclose these facts, in light of the representations made, was, and is, a deceptive practice.

Count 2

16. Through the means described in Paragraph 13, respondent has represented, expressly or by implication, that information transmitted by the Toolbar would be encrypted in transit.

17. In truth and in fact, as described in Paragraph 10, information transmitted by the Toolbar was not encrypted in transit. Therefore, the representation set forth in paragraph 13 was, and is, false or misleading and constitutes a deceptive act or practice.

Count 3

18. Through the means described in Paragraphs 12 and 13, respondent has represented, expressly or by implication, that it employs reasonable and appropriate measures to protect data obtained from consumers from unauthorized access.

19. In truth and in fact, as described in Paragraph 14, respondent did not implement reasonable and appropriate measures to protect data obtained from consumers from unauthorized access. Therefore, the representations set forth in Paragraphs 12 and 13 were, and are, false or misleading and constitutes a deceptive act or practice.

Count 4

20. As described in Paragraphs 9, 10, and 14, respondent'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 – caused or was likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

21. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this twenty-seventh day of March, 2012, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary