

Complaint

IN THE MATTER OF

UPROMISE, INC.CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket No. C-4351; File No. 102 3116
Complaint, March 27, 2012 – Decision, March 27, 2012

This consent order addresses Upromise, Inc.'s advertising, marketing, and operation of an optional feature of that Toolbar, the "personalized offers" feature. 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 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 consent 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.

Participants

For the *Commission*: Katrina Blodgett and Ruth Yodaiken.

For the *Respondent*: J. Beckwith ("Becky") Burr, Wilmer Cutler Pickering Hale and Dorr LLP.

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.

Complaint

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

Complaint

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 TurboSaverTM 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 TurboSaverTM Privacy Statement also stated that “every commercially viable effort” would be made

Complaint

“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.

Complaint

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,

Complaint

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.

Complaint

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.

Complaint

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

By the Commission.

Exhibit 1

Already a member? [Login now](#) | [What is Upromise?](#) | [Schools Program](#)

upromise | [earn](#) | [save](#) | [pay](#) | [family & friends](#) | [resource center](#)

TURBO SAVER | **MAXIMIZE your Upromise savings with the power of TurboSaver™!**

TurboSaver is your online savings reminder.
It alerts you of college savings opportunities when you book travel or shop online.

- Highlights Upromise partners in **Google** and **Yahoo!** search results
- Notifies you of Upromise savings opportunities when you visit partner sites

DOWNLOAD TurboSaver NOW

It's free and installs in seconds.
Requires Microsoft Internet Explorer 6.x, 7.x or 8.x on Windows XP or Windows Vista

By installing the Upromise TurboSaver, you give Upromise permission to direct your visits to Upromise online retailers through your Upromise account and, if you are not logged in as a Upromise member, to request that you log in to your Upromise account before proceeding to the retailer's web site. This is done to ensure that you receive college savings when shopping online.

The following Upromise Online Shopping partners are not compatible with the Upromise TurboSaver: eBay.com, Express, InterContinental Hotels, and Overstock.com. This list is subject to change at any time without notice. To earn a Upromise contribution with these partners, shop directly through upromise.com.

You must install TurboSaver on each web browser you use. If you use both IE and Firefox you should install it on each browser (.exe for IE and .xpi for Firefox).

All Upromise Online Shopping Terms and Conditions apply when using TurboSaver. The [Terms & Conditions](#) and [FAQs](#) can be found in the [Program Details](#). Specific Terms & Conditions apply for each company's contributions and can be found in the Program Details or by clicking on the "store info" popup for that company. Participating companies, contribution levels, and terms and conditions are subject to change without notice.

As part of its functionality, TurboSaver will place icons next to organic search results on Google and Yahoo that identify Upromise participating merchants.

[About Upromise](#) | [Privacy](#) | [Terms and Conditions](#) | [Site Security](#) | [Contact Us](#) | [Careers](#)
[Partnership Opportunities](#) | [Affiliate Program](#) | [Upromise Credit Cards](#) | [Stores and Deals](#) | [Coupons and Offers](#)

© 2001-2009 Upromise, Inc. All rights reserved.
 SLM Corporation and its subsidiaries, including Sallie Mae, Inc. and Upromise, Inc., are not sponsored by or agencies of the United States.
 ‡ Securities offered through Upromise Investments, Inc. (member FINRA)

Complaint

Exhibit 2

Complaint

Exhibit 3

close X



Install TurboSaver™

and get college savings when you shop online.

By pressing install now, I agree to the [TurboSaver license agreement](#) and to download TurboSaver on to my computer.

License Agreement

Upromise TurboSaver™ End User License Agreement

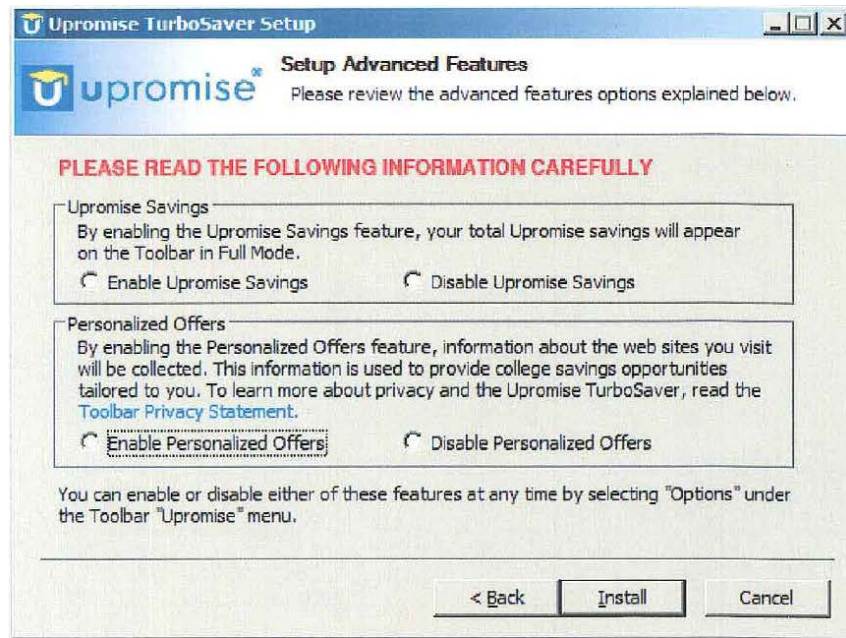
Thank you for using the Upromise TurboSaver™, a savings tool. BY DOWNLOADING, INSTALLING OR USING THIS SOFTWARE, INCLUDING ANY THIRD PARTY SOFTWARE MADE AVAILABLE IN CONJUNCTION WITH THIS SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT BETWEEN YOU AND UPROMISE, INC. THE TERM "SOFTWARE", AS USED IN THIS AGREEMENT, ALSO INCLUDES ANY

☐ **Enable Personalized Offers (optional)**

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.

install now »

Complaint

Exhibit 4

Complaint

Exhibit 5

Upromise TurboSaver™ Privacy Statement

Introduction

We understand and respect that you are concerned about your privacy. Protecting your privacy is a top priority at Upromise. We want you to know that if you choose to enable the Personalized Offers feature of the Upromise TurboSaver, information about the web sites you visit will automatically be forwarded to Upromise or our service provider. This Upromise TurboSaver Privacy Statement is intended to explain to you the type of information being collected and the way that information may be used or shared.

Your Choice

Information about the web sites you visit will only be collected if you make an explicit choice to enable the Personalized Offers feature of the Upromise TurboSaver. Enabling Personalized Offers mean that you'll occasionally see windows slide up your screen reminding you of relevant Upromise partners or programs. You are not signing up for any email or regular mail of any kind.

During the installation of the Upromise TurboSaver, you will be asked if you would like to enable or disable the Personalized Offers feature. After installation, you may choose to enable or disable the Personalized Offers feature at any time by selecting "Options" under the TurboSaver's "Upromise" menu.

Information Collected

When you enable the Personalized Offers feature, either we or our service provider collects what is known as "Click Stream Data." Click Stream Data is anonymous, and includes information such as your IP address URLs of web pages that you have viewed, and the date that you viewed the web pages.

Infrequently, the Click Stream Data collected may inadvertently contain personal information. Potentially, a name, address, email address, or similar information that you enter into a web page can become part of the Click Stream Data that is transmitted to and stored by our service provider. Our service provider makes every commercially viable effort to purge their databases of any personally identifiable information. Before the Click Stream Data is transmitted to and stored by our service provider a proprietary rules engine is used to search through the Click Stream Data and remove any personally identifiable information. Our service provider is contractually bound not to use the data collected through the Personalized Offers feature for any purpose other than to assist us in the operation of the Upromise Service or the limited use described below under "Sharing with Third Parties."

How Collected Information is Used

We may use the non-personally identifiable information collected through the Personalized Offers feature to help us better target college savings opportunities and other content to you in an effort to create a personally relevant experience. We may also use the non-personally identifiable information collected through the Personalized Offers feature to help us formulate and predict responses to various savings opportunities, and to deliver and help determine the effectiveness of various savings opportunities.

Complaint

We may also combine the information collected through the Personalized Offers feature with personally identifiable data, such as your transaction information, to assist with targeting savings opportunities to your preferences and to help us formulate, predict responses to, deliver and determine the effectiveness of various savings opportunities.

Sharing with Third Parties

We may share the non-personally identifiable data collected through the Personalized Offers feature on an anonymous and aggregate basis with third parties, including our contributing companies, to formulate, predict responses to, deliver and determine the effectiveness of various savings opportunities. In addition, our service provider may use the non-personally identifiable data collected through the Personalized Offers feature on an anonymous and aggregate basis to provide online consumer research services for others. For more information view our service provider's [Privacy Policy](#).

More Information

The Upromise TurboSaver will periodically contact servers at Upromise to download updated configuration files. These files control the advanced features of the tool, including the "Specials" menu and the feature that allows you to receive college savings when shopping online at most Upromise partners, even if you forgot to start your online shopping at Upromise.com.

In addition, the Upromise TurboSaver will periodically contact servers at our service provider to see if you are running the most current version. If necessary, you will automatically be provided with the latest update to the Upromise TurboSaver.

We hope that you find this privacy statement helpful and understand the benefits associated with your use of the Upromise TurboSaver's Personalized Offers feature. If you feel that the benefits of using the Personalized Offers feature do not outweigh the information that we collect, you should choose not to enable the Personalized Offers feature.

For more information about Upromise's full privacy policy, click [here](#).

Complaint

Exhibit 6

Upromise Privacy Statement

Protecting your privacy is a top priority at Upromise. We want you to understand how we handle the personal information about you that we may obtain, and how we may and may not share it. This statement covers all of our information handling practices for Upromise, Inc. and its subsidiaries, including Upromise Investments, Inc. and Upromise Investment Advisors, LLC, for the benefit of current and past customers. Please also see our separate statement, [Privacy of Upromise Rewards Service](#), for additional information about our practices relating to our Rewards service.

Information We May Obtain.

As part of providing you products or services, we may obtain personal information from the following sources:

- **Information you provide to us** on applications and other forms, that you otherwise enter on our web site, or that you provide to us in writing or by telephone, such as when you contact our customer service staff. This information may include items such as your name, address, telephone number and social security number. In addition, please see **Use of Cookies and other Technologies** below for information we receive automatically when you visit our web site.
- **Information from your transactions** with us, our affiliates or nonaffiliated third parties such as account activity and your purchase information in our Rewards service.
- **Information from third parties**, including public sources, such as verification services and consumer reporting agencies (to comply with regulatory requirements, ensure the accuracy of data and prevent fraud, for example), or from other sources (such as from other institutions like a bank or broker you use to transfer funds into a Upromise account, or public sources).

We use the information we obtain in order to develop, offer and deliver our products and services, to offer products and services of our affiliates, participating companies, marketing partners and other companies, to process transactions in your accounts, and to fulfill legal and regulatory requirements.

Please note that information you voluntarily include in bulletin boards, chat rooms and other online forums, such as the Upromise Community, may be viewed and used by anyone with access to those forums. Upromise is unable to control any use of such information.

Sharing Information With Our Affiliates

As a subsidiary of SLM Corporation, commonly known as Sallie Mae, our affiliates are the family of companies controlled by SLM Corporation. Our affiliates include, among others, Sallie Mae, Inc., Upromise Investments, Inc., Upromise Investment Advisors, LLC, Student Loan Funding Resources, Nellie Mae Corporation, Southwest Student Services Corporation, Student Loan Finance Association, Academic Management Services Corp., SLM Financial Corporation, and Sallie Mae Bank. Our affiliates offer a broad range of products and services including education loans, private loans, mortgage loans, 529 college savings plan administrative services and debt collection services. By sharing your personal information with our affiliates, we and our affiliates can better understand and meet your college savings and other needs by letting you know about products, services and promotional offers in which you are most likely to be interested. For example, if you have a Rewards account that has accumulated sufficient funds, you may be interested in opening an account with the Upromise College Fund, or if you have a high school student, you may be interested in learning more about Sallie Mae student loans.

Unless you tell us not to, we may share with our affiliates all of the information we obtain about

Complaint

you. If you prefer that we not share with our affiliates consumer report information about you that we may receive from third parties, you may direct us not to do so by sending us an email at customercare@upromise.com containing your name, address, account number and request, or by calling the following toll free number: 1-800-877-6647. Please be aware that we may continue to share any other information as permitted by law.

Sharing Information With Nonaffiliated Third Parties

Information about our customers is an important part of our business. We do not share your personal information with nonaffiliated third parties except as permitted or required by law, including as provided below:

- **Agents and Service Providers.** In order to provide our products and services, we may share personal information about you with agents and service providers to perform functions on our behalf, such as to send email and postal mail, analyze data, provide marketing services, process applications and credit card payments, and service accounts. We contractually obligate these service providers to access and use personal information only as needed to perform their functions and for no other purposes.
- **Financial Services Providers.** In order to make certain financial products available to you (for example, credit cards, loans or insurance), we sometimes enter into marketing agreements with nonaffiliated financial institutions that offer those products. We select the financial institutions we work with very carefully. Generally, we provide these entities with only customer contact information. For some products, we might also provide them limited additional information. These entities are permitted to use the information we give them only for the specific products being offered under our contract. If you prefer that we do not share your information with nonaffiliated financial institutions so that they may market their products and services directly to you, you may opt-out of that information sharing by sending us an email at customercare@upromise.com containing your name, address, account number and request, or by calling the following toll free number: 1-800-877-6647. You may also opt-out of that information sharing by updating your Upromise account member profile opt-out preferences on our website to opt-out of receiving communications from our participating companies.
- **Protection of Upromise and Others.** We may disclose personal information about you to third parties when we believe such disclosure is appropriate to comply with a legal requirement, such as a law, regulation, court order, subpoena or search warrant, or in the course of a legal proceeding. We may also disclose personal information as we believe appropriate to enforce or apply our rights under our agreements with customers, to protect the rights, property or safety of Upromise, our customers and others, including exchanging information for fraud protection and credit risk reduction.
- **Business Transfers.** If there is a change of control in Upromise's business (whether by merger, sale, or otherwise), its customer information could be sold as part of that transaction and your personally identifying information potentially could be used by the purchaser. Notice will be posted on the website so that you are aware of this change of control.

Upromise does not share member information with nonaffiliated, non-financial institutions to enable them to market their products and services directly to you. Occasionally, we engage third party service providers in the business of facilitating communications to send you information from certain participating companies, but only subject to strict confidentiality provisions that prohibit those third parties from providing your personal information to the participating companies. If we ever make the decision to share member information with nonaffiliated third parties other than financial institutions as described above so that they may market their products and services directly to you, we will notify you ahead of time, and you will have the opportunity to opt-out of that information sharing.

Use of Cookies and other Technologies

Complaint

Our web servers place and read "cookies" on our site's visitors' web browser for a variety of purposes. Cookies are small data files that are stored on an Internet user's web browser by a web server. One important use of cookies is to help identify you while you are logged in to the Upromise site. Consequently, if your browser does not accept session cookies, you will be unable to enroll or log in to our service using our site. You will, however, be able to browse our site as a visitor. The information Upromise collects from cookies and web server logs is used to administer the web service and customize information you receive when visiting our site. Upromise may also use and share aggregate information from cookies and web server logs to analyze and improve our web service offerings. This information does not identify individual visitors or customers.

As is true of most web sites, we gather certain information automatically and store it in log files. This information includes the internet protocol (IP) addresses, browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp, and clickstream data. We use this information to analyze trends, to administer our web site, to track users' movements around the web site and to gather demographic information about our user base as a whole. We, certain third parties who host portions of our web site, and certain advertising affiliates or others employ cookies and/or small pieces of code known as "web beacons" or "clear gifs" that, on an anonymous basis, count users that have visited a page that contains these web beacons. We use web beacons to help us better manage content on our site and to determine which content is effective. In addition, third party advertising affiliates and others may use web beacons to help us track the effectiveness of our advertisements placed on third party web sites. Web beacons on our site are not used to collect personally identifiable information about our customers. Finally, we use web beacons in our HTML-based emails to let us know which emails have been opened by recipients so that we may gauge the effectiveness of our communications. If you would like to opt-out of these emails, please see "Choices Regarding the Receipt of Marketing Messages."

If you have not opted-out of receiving marketing messages from us about our products and services, we may use information from our log files, cookies or web beacons to help us make those communications more useful or interesting to you.

One of our third party service providers that uses these technologies to assist us in tracking site usage is Coremetrics. As a result of your accessing our site, Coremetrics may on our behalf collect information about you. This service allows us to better provide our product or service to you. Coremetrics does not have the right to use the information they receive beyond what is necessary to assist us. For further information, including how to opt out, consult Coremetrics' privacy policies at: www.coremetrics.com/info_eluminate2.html.

Choices Regarding the Receipt of Marketing Messages

You may choose whether and to what extent you receive marketing messages from Upromise about products and services offered by Upromise or third parties. You may also choose whether and to what extent you receive marketing messages from our participating companies based on our information. If you do not wish to receive any of these marketing messages, you may opt out. And we offer you choices, so that you may elect to receive offers that are of interest to you in the ways you wish. If you do not wish to receive marketing messages, you may opt out by sending us an email at customercare@upromise.com containing your name, address, account number and request, or by contacting a customer service representative at 1-800-877-6647. You may also opt-out of receiving marketing emails from Upromise and marketing messages from our participating companies, by updating your Upromise account member profile opt-out preferences on our web site. We reserve the right to send you specific administrative notices that are required by law, regulation, or as needed to service your account. In addition, our participating companies reserve the right to contact you using information from sources other than Upromise.

Security of Your Personal Information

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. The only Upromise employees who are authorized to see your personal information are those who need it as part of their jobs.

Complaint

Please remember that you also play a valuable part in data security. You should never share your Upromise password with anyone. If you feel your password has been compromised, you should change it immediately. After you have finished using our site, you should log out of your Upromise account and exit your browser so that no unauthorized persons can use our site under your name and account information.

Collection of Information from Children.

None of Upromise's products or services are intended for purchase by children. Accordingly, Upromise does not knowingly collect, either online or offline, personally identifiable information from children under the age of 13.

State Laws

In addition to the rights described in this policy, please note that you may have additional rights under state law. For example, if your address on file with us is a California address, we will not share personal information about you with a financial institution with whom we have a joint marketing relationship unless we provide you the required notice under California law and you do not opt-out of that information sharing. In addition, if your address on file with us is a Vermont address, we will not share consumer report information about you with our affiliates unless you expressly consent to that information sharing.

Changes to This Privacy Statement

If we materially change this statement or our information-handling practices as described in this statement, we will notify you by email and/or through a notice on our web site at least 30 days prior to their implementation.

Privacy of Upromise Rewards Service

What information does Upromise collect, and why?

Enrollment Information. To set up your membership with the Upromise Rewards service, you will need to provide certain contact information, such as your name, mailing address, email address, phone number, username, and password. This information will also allow us to contact you about new college savings opportunities, unless you opt out of receiving these messages.

Purchase Information. As a Rewards service member, you can save for college by shopping with our participating companies. We may require additional information in order to keep track of and collect your contributions. For example, if you use a credit card to make a purchase, we may use your credit card number to identify the transaction. A phone company might require your telephone number, while an airline might require your frequent flyer account number. To take part in our grocery service, you may need to provide a grocery loyalty card number. In order to keep track of and collect your contributions, Upromise collects from some participating companies, grocery retailers or third party processors details of your transactions such as the date and amount of your transaction.

Rewards Account Information. We will maintain records to keep track of the contributions you earn from your purchases with our participating companies. You can use our website to view your Rewards service account balances and recent account activities, update your account profile, establish college savings goals, add new future college students, or contact a customer service representative.

Student Information. In order to link an eligible investment account or student loan account to the Rewards service so that we may direct your savings from your Rewards service account to the investment or student loan account you will need to provide certain information about the students or future students for whom you are saving such as the name, date of birth and social security

Complaint

number of the student and the account number of the investment or loan account. You can also personalize your Rewards service account to reflect your progress toward achieving your personal college savings goals by providing additional information about your future college students, such as when they anticipate starting college and whether they plan to attend a public or private institution. We may use this information to contact you about college savings opportunities, unless you opt out of receiving these messages.

Investment Account Information. When you open an investment account, the investment manager is required by law and by industry regulations to obtain certain personal information before creating your investment account. We and our investment manager partners will share certain personal information (such as your or your student's social security number or address) and demographic data with one another to facilitate the application process and monthly processing, and to comply with applicable law. This sharing of information is required to manage your account. Additionally, we may use this demographic information (such as your future college student's date of birth) to contact you about relevant college savings opportunities, unless you opt out of receiving such messages.

Family and Friends Network Information. You may use our Tell-a-Friend service to notify your family and friends about Upromise by providing their names and email addresses. You can also increase your college savings through Upromise by creating a savings network of family and friends that directs a portion of its Upromise savings to your future college students.

Upromise will automatically send a one-time email inviting your family and friends to visit Upromise. We store the information for the purpose of sending these emails and to measure overall response rates to these services. Your family and friends may [contact us](#) to request that their information be removed.

Family and friends who contribute to your future college students' investment accounts will receive confirmation of the name and age of each future college student for whom they are saving.

How does Upromise use my information?

Management of Your Account. When you become a member, we use your contact and transaction data to manage your account.

Use of Third Parties for Fulfillment Purposes. We may use certain third parties to provide marketing and administrative services, such as keeping track of your purchases, analyzing data or delivering special college saving offers to you on our behalf or on behalf of our participating companies. Third parties may also be used to help us administer our grocery, dining, travel and other rewards programs. In order to obtain these services, we may need to share certain personally identifiable information about our members. However, these third parties will be bound by legal agreements to not use or disclose the information we provide them for any purpose other than to perform the requested service.

On occasion, contests, sweepstakes or surveys on our web site may be co-sponsored by Upromise and another company, or may be sponsored by companies other than Upromise. Some or all of the data collected through these contests, sweepstakes or surveys may be shared with the sponsor(s) or companies indicated on the entry form or in the applicable rules.

Notification About Products and Services. We offer you the chance to maximize your Upromise membership through opportunities made available to you on our site and, unless you opt out of receiving them, through email, mail, and telephone messages. We may use information about you to provide you offers tailored to your interests. Sometimes, we send offers to selected groups of members on behalf of our participating companies and/or affiliates. Occasionally, we engage third parties in the business of facilitating communications to send you information from certain participating companies, but only subject to strict confidentiality provisions that prohibit those third parties from providing your personal information to the participating companies. In addition, unless you opt-out, we may share your information with nonaffiliated financial institutions with whom we have a marketing relationship so that those participating companies may market to you the specific products being offered under our contract with them. If you do not want to receive any of these marketing communications, you may opt out of receiving them.

Complaint

Use of Information from Third Parties. We may obtain information about you from our participating companies and other third parties in order to provide you with college savings opportunities tailored to your interests. You may opt out of receiving these offers by updating your account profile at any time on our website, or by contacting a customer service representative at 1-800-877-6647. We may also use information obtained from our participating companies and other third parties in conjunction with member account and enrollment information for analytical and audit purposes.

Use of Non-Personally Identifiable Information. We may also provide aggregated, non-personally identifiable information about our members and their future college students to third parties for audit, marketing and other purposes. Because aggregated data is not associated with any particular person, these third parties will not have access to any personally identifiable information about you or your future college students.

What are my choices regarding the receipt of marketing messages?

We reserve the right to send you specific administrative notices that are required by law, regulation, or as needed to service your account. You may choose whether or not to receive messages from Upromise and our participating companies that may better suit your interests based on your preferences and transaction history. If you do not wish to receive these messages from Upromise and/or our participating companies, you may opt out by sending us an email at customercare@upromise.com containing your name, address, account number and request, or by calling the following toll free number: 1-800-877-6647. You may also opt-out of receiving marketing emails from Upromise and marketing messages from our participating companies by updating your Upromise account member profile opt-out preferences on our web site. Our participating companies reserve the right to contact you using information from sources other than Upromise.

How can I access and update my Upromise data?

You may access and update information stored in your account profile by visiting the Upromise site. Please keep your contact, account, and preference information up-to-date. Doing so ensures that your contributions are properly tracked and received. It also helps us inform you of new participating companies who may help you boost your college savings.

What about links to other sites and participating companies' use of information?

Through our various online offerings, we may provide links to third-party websites, such as those of our participating companies or your investment manager. Each of these sites may have separate privacy and different data-collection practices from Upromise, and we are not responsible for the actions or practices of these third parties, nor for the content on these sites. We encourage you to review the privacy policies of their sites. In addition, our remindU service and the Personalized Offers feature of the Upromise Toolbar are provided by third parties, which also have separate privacy policies and data-collection practices which can be accessed when you down-load the remindU and Upromise Toolbar software. To learn more about privacy and the Upromise Toolbar, please read the Toolbar Privacy Statement. Finally, please remember that when you shop or do any other business with any of our participating companies, any information you provide to them is subject to their own privacy and data collection practices, for which Upromise is not responsible.

What is TRUSTe and why is it so important?

Upromise, a wholly-owned subsidiary of Sallie Mae, is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to build users' trust and confidence in the Internet by promoting the use of fair information practices. TRUSTe has agreed to review the practices of www.upromise.com because this website wants to demonstrate its commitment to your privacy. Please note that the TRUSTe program does not cover the privacy practices of Upromise, Inc. affiliates. Please also note that the TRUSTe program covers only information that is collected through this website, and does not cover information that may be collected through software downloaded from the site.

If you have questions or concerns regarding this statement, you should first contact Upromise (see below). If you do not receive acknowledgment of your inquiry or your inquiry has not been satisfactorily addressed, you should then contact TRUSTe. TRUSTe will then serve as a liaison with Upromise to resolve your concerns.

Complaint

How do I contact Upromise about this Privacy Statement?

If you have any questions about this privacy statement, our information-handling practices, or other aspects of privacy at Upromise, please [contact us](#) by email or at Upromise, Inc., Customer Care - Privacy Policy Issues, 95 Wells Avenue, Suite 160, Newton, MA 02459.

Last Updated 6-12-08

Complaint

Exhibit 7**Upromise Security Statement**

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:

- Monitoring for intrusion attempts - 24 hours a day, 7 days a week;
- SSL, Data, and Password encryption technology;
- Firewalls and systems monitoring;
- Security audits and inspections by leading security firms.

How Does Upromise Protect Your Security?

The security of your personal information, transactions and savings is our priority at Upromise. Using the Secure Sockets Layer protocol (SSL), Upromise automatically encrypts your sensitive information in transit from your computer to ours. Once your information reaches us, it resides on servers that are configured for maximum security and are continuously monitored for unauthorized changes. Upromise security architecture and security procedures are audited and inspected by industry leaders specializing in security processes and technologies.

How Can You Help Upromise Protect Your Security?**Username and Password**

Choose a password that will be difficult for others to guess. Do not use obvious or easily accessed data such as your name, initials, Social Security number, mother's maiden name, phone number, address, family birthdays, family names, pets, or any combination of the previous. We emphasize the importance of choosing a unique and secure password to help ensure your protection. Upromise will never contact you to solicit your username or password. Never provide them to anyone.

Close Your Browser When Finished

After you have finished your session with Upromise, log out and close your browser to erase information that may have been stored on your computer during your session. Any information you entered during your session may be temporarily stored in the memory storage area of your computer until you close the browser. Logging off and closing your browser will clear this temporary storage area from your computer.

Verify authenticity of emails

Never click on a link in an email if you are unsure of its origins, especially if the email asks for personal or financial information. If you have any doubt about the authenticity of an email from Upromise, simply open a new Web browser, type in <http://www.upromise.com>, log in to your Upromise account safely and securely and then perform the requested activity.

Decision and Order

DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft of Complaint which the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the Respondent with violation of the Federal Trade Commission Act; and

The Respondent and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of the agreement is for settlement purposes only and does not constitute an admission by the Respondent that the law has been violated as alleged in such complaint, or that any of the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the Respondent has violated the Federal Trade Commission Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comment received from an interested person pursuant to Section 2.34 of its Rules, now in further conformity with the procedure prescribed in Section 2.34 of its Rules, 16 C.F.R. § 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following order:

1. Respondent Upromise, Inc., is a Delaware corporation with its principal office at 95 Wells Avenue, Suite 160, Newton, Massachusetts 02459.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the

Decision and Order

Respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

For purposes of this order, the following definitions shall apply:

- A. “Affected Consumers” shall mean persons who, prior to the date of issuance of this order, downloaded and installed the TurboSaver Toolbar and had the Personalized Offers feature enabled.
- B. “Clearly and prominently” shall mean as follows:
 - 1. In textual communications (*e.g.*, printed publications or words displayed on the screen of a computer or a mobile device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;
 - 2. In communications disseminated orally or through audible means (*e.g.*, radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;
 - 3. In communications disseminated through video means (*e.g.*, television or streaming video), the required disclosures are in writing in a form consistent with subparagraph (A) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication;

Decision and Order

4. In communications made through interactive media, such as the Internet, online services, and software, the required disclosures are unavoidable and presented in a form consistent with subparagraph (A) of this definition, in addition to any audio or video presentation of them; and
 5. In all instances, the required disclosures are presented in an understandable language and syntax, and with nothing contrary to, inconsistent with, or in mitigation of the disclosures used in any communication of them.
- C. “Collected Information” shall mean any information or data transmitted from a computer by the TurboSaver Toolbar as a result of the Personalized Offers feature being enabled prior to the date of issuance of this order to any computer server owned by, operated by, or operated for the benefit of respondent.
- D. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
- E. “Computer” shall mean any desktop or laptop computer, handheld device, telephone, or other electronic product or device that has a platform on which to download, install, or run any software program, code, script, or other content and to play any digital audio, visual, or audiovisual content.
- F. “Covered Online Service” shall mean any product or service using or incorporating a Targeting Tool. Covered Online Service includes, but is not limited to, the TurboSaver Toolbar with the Personalized Offers feature enabled.
- G. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an

Decision and Order

email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver's license number or other government-issued identification number; (g) prescription information, such as medication and dosage, and prescribing physician name, address, and telephone number, health insurer name, insurance account number, or insurance policy number; (h) a bank account, debit card, or credit card account number; (i) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; (j) a biometric record; or (k) any information that is combined with any of (a) through (j) above.

- H. "Personalized Offers feature" shall mean the component of the TurboSaver Toolbar that Upromise has offered under the name of "Personalized Offers."
- I. "Respondent" shall mean Upromise, Inc., and its successors and assigns, and its officers, agents, representatives, and employees.
- J. "Targeting Tool" shall mean any software program or application distributed by or on behalf of respondent that is installed on a consumer's computer, whether as a standalone product or as a feature of another product, and used by or on behalf of respondent to record or transmit information about any activity occurring on that computer involving the computer's interactions with websites, services, applications, or forms, unless (a) the activity involves transmission of information related to the configuration of the software program or application itself; (b) the activity involves a consumer's interactions with respondent's websites, services, applications, and/or forms; or (c) the activity involves a consumer's interactions with respondent's member merchants and that information is collected, retained, or used only as necessary for the purpose of

Decision and Order

providing the consumer's reward service benefits for transactions involving those merchants.

The TurboSaver Toolbar when configured to collect consumer data, for example, with the Personalized Offers feature enabled, is a Targeting Tool.

- K. "Third party" shall mean any individual or entity other than respondent, except that a third party shall not include a service provider of respondent that:
1. only uses or receives personal information collected by or on behalf of respondent for and at the direction of the respondent and no other individual or entity,
 2. does not disclose the data, or any individually identifiable information derived from such data, to any individual or entity other than respondent, and
 3. does not use the data for any other purpose.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, website, or other device, in connection with the advertising, promotion, offering for sale, sale, or distribution of any Targeting Tool, in or affecting commerce, shall,

- A. Prior to the consumer enabling (by downloading, installing, or otherwise activating) any Targeting Tool:
1. Clearly and prominently, and prior to the display of and on a separate screen from, any "end user license agreement," "privacy policy," "terms of use" page, or similar document, disclose:
 - a. all the types of data that the Targeting Tool will collect, including but not limited to, if applicable, a statement that the data includes transactions or communications between the

Decision and Order

consumer and third parties in secure sessions, interactions with shopping baskets, application forms, online accounts, web-based email accounts, or search engine pages, and if the information includes personal, financial or health information.

- b. how the data is used, including if the data is shared with a third party, other than as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, (ii) to enforce respondent's terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.
 - 2. Obtain express affirmative consent from the consumer to the enabling (by downloading, installing, or otherwise activating) and to the collection of data.
- B. For those TurboSaver Toolbars installed by consumers before the date of issuance of this order, prior to (1) enabling data collection through any Targeting Tool or (2) otherwise making any material change from stated practices about collection or sharing of personal information through the TurboSaverToolbar, provide the notice and obtain the express consent described in subparts A(1) and (2) of this Part.

II.

IT IS FURTHER ORDERED that respondent shall:

- A. Notify Affected Consumers: a) that they have or had the Personalized Offers feature enabled, and that from 2005 through January 2010 use of this feature resulted in collection and transmission of data to or on behalf of respondent, listing the categories of personal information that were, or could have been, transmitted; and b) how to permanently disable the Personalized Offers feature and uninstall the TurboSaver Toolbar. Notification shall be by each of the following means:

Decision and Order

1. Beginning within thirty (30) days after the date of service of this order and for two (2) years after the date of service of this order, posting of a clear and prominent notice on its website.
 2. Beginning within thirty (30) days after the date of service of this order and for three (3) years after the date of service of this order, informing Affected Consumers who complain or inquire about the privacy or security of the TurboSaver Toolbar.
 3. Within sixty (60) days after the date of service of this order, providing direct, clear and prominent notice to Affected Consumers who have the Personalized Offers feature enabled.
- B. Provide prompt, toll-free, telephonic and electronic mail support to help Affected Consumers disable the Personalized Offers feature and, if requested, uninstall the TurboSaver Toolbar.

III.

IT IS FURTHER ORDERED that respondent shall, within five (5) days after the date of service of this order, delete or destroy, or cause to be deleted or destroyed, all Collected Information in respondent's custody or control, unless otherwise directed by a representative of the Commission.

IV.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, website, or other device, in connection with its advertising, marketing, promotion, or offering of any service or product in or affecting commerce, shall not make any representation, in any manner, expressly or by implication, about the extent to which respondent maintains and protects the security, privacy, confidentiality, or integrity of any personal information collected from or about consumers, unless the representation is true, and non-misleading.

Decision and Order

V.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, website, or other device, in connection with its advertising, marketing, promotion, or offering of any product or service, in or affecting commerce, shall maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of personal information collected from or about consumers. This section may be satisfied through the review and maintenance of an existing program so long as that program fulfills the requirements set forth herein. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity and the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. The designation of an employee or employees to coordinate and be accountable for the information security program;
- B. The identification of material internal and external risks that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of personal information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, account takeovers, or other systems failures;
- C. The design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the

Decision and Order

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

- D. The development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information such service providers receive from respondent or obtain on respondent's behalf, and the requirement, by contract, that such service providers implement and maintain appropriate safeguards; and
- E. The evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

VI.

IT IS FURTHER ORDERED that, in connection with its compliance with Part V of this order, for any Covered Online Service respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

Decision and Order

- A. Set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. Explain how such safeguards are appropriate to respondent's size and complexity, and the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;
- C. Explain how the safeguards that have been implemented meet or exceed the protections required by Part V of this order; and
- D. Certify that respondent's 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.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

VII.

IT IS FURTHER ORDERED that respondent shall, for a period of five (5) years after the last date of dissemination of any representation covered by this order, maintain and upon request make available to the Commission for inspection and copying:

- A. All advertisements, labeling, packaging and promotional material containing the representation;

Decision and Order

- B. All materials relied upon in disseminating the representation;
- C. All tests, reports, studies, surveys, demonstrations, or other evidence in its possession or control that contradict, qualify, or call into question the representation, or the basis relied upon for the representation, including complaints and other communications with consumers or with governmental or consumer protection organizations; and
- D. All acknowledgments of receipt of this order, obtained pursuant to Part IX.

Moreover, for a period of three (3) years after the date of preparation of each Assessment required under Part VI of this order, respondent shall maintain and upon request make available to the Commission for inspection and copying all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

VIII.

IT IS FURTHER ORDERED that respondent shall, 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 Commission's complaint, cooperate in good faith with the Commission and appear at such places and times as the Commission shall reasonably request, after written notice, for interviews, conferences, pretrial discovery, review of documents, and for such other matters as may be reasonably requested by the Commission. If requested in writing by the Commission, respondent shall appear and provide truthful testimony in any trial, deposition, or other proceeding related to or associated with the transactions or the occurrences that are the subject of the complaint, without the service of a subpoena.

Decision and Order

IX.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to: (1) all current and future principals, officers, and directors; and (2) all current and future managers who have responsibilities with respect to the subject matter of this order, and shall secure from each such person a signed and dated statement acknowledging receipt of the order, with any electronic signatures complying with the requirements of the E-Sign Act, 15 U.S.C. § 7001 *et seq.* Respondent shall deliver this order to current personnel within thirty (30) days after the date of service of the order, and to future personnel within thirty (30) days after the person assumes such position or responsibilities.

X.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary (including an LLC), parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in respondent's name or address. *Provided, however,* that with respect to any proposed change about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge.

Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, with the subject line FTC v. Upromise. *Provided, however,* that, in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of such notices is contemporaneously sent to the Commission at Debrief@ftc.gov.

Decision and Order

XI.

IT IS FURTHER ORDERED that respondent shall, within sixty (60) days after service of this order, and at such other times as the FTC may require, file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form in which respondent has complied with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, respondent shall submit additional true and accurate written reports.

XII.

This order will terminate on December 31, 2031, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Part of this order that terminates in less than twenty (20) years;
- B. This order's application to any respondent that is not named as a defendant in such complaint; and
- C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that the respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that this order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Analysis to Aid Public Comment

**ANALYSIS OF CONSENT ORDER TO AID PUBLIC
COMMENT**

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

LONG FENCE & HOME, LLLPCONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket No. C-4352; File No. 112 3005
Complaint, April 5, 2012 – Decision, April 5, 2012

This consent order addresses Long Fence & Home, LLLP's marketing and sale of replacement windows for use in residences. The complaint alleges that respondent did not possess and rely upon a reasonable basis substantiating the representations that consumers who replace their windows with Long Windows' Quantum2 replacement windows with SuperPak Glass are likely to achieve residential energy savings of 50% or save 50% on residential heating and cooling costs. The consent order prohibits respondent from making any representation that: (A) consumers who replace their windows with respondent's windows achieve up to or a specified amount or percentage of energy savings or reduction in heating and cooling costs; or (B) respondent guarantees or pledges that consumers who replace their windows with respondent's windows will achieve up to or a specified amount or percentage of energy savings or reduction in heating and cooling costs; unless the representation is non-misleading and, at the time of making such representation, respondent possesses and relies upon competent and reliable scientific evidence to substantiate that all or almost all consumers are likely to receive the maximum represented savings or reduction.

Participants

For the *Commission: Robert Frisby, Zachary Hunter, Joshua Millard, and Sarah Waldrop.*

For the *Respondent: D.S. Berenson, Johanson Berenson LLP.*

COMPLAINT

The Federal Trade Commission, having reason to believe that Long Fence & Home, LLLP ("respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Long Fence is a Maryland limited liability limited partnership with its principal office or place of business at 10236 Southard Drive, Beltsville, Maryland 20705. Respondent