**102 3155**

**UNITED STATES OF AMERICA**
**BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:** **Jon Leibowitz, Chairman**
**Edith Ramirez**
**Julie Brill**
**Maureen K. Ohlhausen**
**Joshua D. Wright**

| | | |
|---|---|---|
| **In the Matter of** | ) | |
| **COMPETE, INC.,** **a corporation.** | ) | **DOCKET NO. C-4384** |

## COMPLAINT

The Federal Trade Commission, having reason to believe that Compete, Inc. ("Compete" 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. Compete is a Delaware corporation, with its principal place of business at 501 Boylston Street, Suite 6101, Boston, Massachusetts.

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. Compete is a market research company that collects data from consumers so that it can, among other things, develop and sell analytical reports about consumer behavior on the Internet.

4. Starting in January 2006, Compete collected data about consumers through two products. The first was the Compete Toolbar ("Toolbar"), which consumers installed to get "instant access" to information about websites as they surfed the Internet, such as the popularity

of the websites they visited. (*See* Compete Toolbar, Exhibit 1, formerly available from www.compete.com). The second product was the Consumer Input Panel, which allowed consumers to win rewards while expressing their opinions to companies about products and services. (*See* Consumer Input Panel, Exhibit 2, formerly available from www.consumerinput.com).

5. In addition, Compete licensed its data collection software for third parties for their use, including incorporating into their own toolbars or rewards programs. In all cases the data gathered through Compete's data collection software was sent to Compete.

6. As of the end of October 2011, Compete had collected data from more than 4 million consumers.

**Compete's Tracking of Consumers' Activities**

7. When consumers installed the Toolbar, they were prompted to either leave enabled or to disable a feature the company referred to as "Community Share." (*See* Exhibit 3). Compete provided the following description of the "Community Share" option:

> By joining Community Share, the web pages you visit will be anonymously pooled with the Compete community to provide site trust rankings and analytics.
>
> *See* Compete Toolbar Setup, Exhibit 3.

Enabling "Community Share" activated Compete's ability to collect data about the consumer.

8. When consumers signed up for the Consumer Input Panel, Compete made statements such as the following:

> [W]e measure your behavior as well as your opinions. Consumer Input utilizes a piece of software stored on your computer that anonymously transmits aspects of your Internet browsing behavior so that we can understand the sites, products and services you interact with.
>
> *See, e.g.,* Consumer Input Panel Registration, Exhibit 4.

Compete always collected data about consumers who participated in the Consumer Input Panel.

9. In addition, in its general privacy policy, Compete made the following statement about "click-sharing," which refers to the consumers' sharing of data with Compete:

> When you download Compete software, including the Compete Toolbar, you will be given the option of enabling click-sharing. Should you opt-in to click-sharing you will begin to anonymously share the addresses of the web pages you visit online.
>
> *See* General Compete Privacy Policy, Exhibit 5.

10. In fact, Compete collected more than browsing behavior or addresses of web pages. It collected extensive information about consumers' online activities and transmitted the information in clear readable text to Compete's servers. The data collected included information about all websites visited, all links followed, and the advertisements displayed when the consumer was on a given web page. The captured data included details about consumers' online behavior to the extent that, for example, Compete knew whether a consumer abandoned or completed a purchase after placing an item in an online shopping cart.

11. Moreover, as far back as January 2006, Compete also captured some information consumers communicated on secure web pages (e.g., https), such as credit card numbers, financial account numbers, security codes and expiration dates, usernames, passwords, search terms, or Social Security numbers.

12. Compete's data capture occurred in the background as a consumer used the Internet; there was no way for consumers – without special software and technical expertise – to discover the extent of the data collection.

**Compete's Filtering of Consumer Data**

13. Compete made statements in its general privacy policy about filtering of personal information such as the following:

> All data is stripped of personally identifiable information before it is transmitted to our servers. Our data collection techniques have been designed to purge personally identifiable information wherever we find it. In addition, as a member of Compete you are assigned a randomly generated user ID ensuring your anonymity.
>
> *See* General Compete Privacy Policy, Exhibit 5.

14. Similarly, Compete made statements in its Consumer Input Panel privacy policy and Frequently Asked Questions such as the following:

> Inadvertently, the URL information we collect and license sometimes contains personal information about Internet users. Potentially, a name, address, email address, or similar information that an Internet

> user enters into a Web page can become part of the URL that is transmitted to us and stored in our databases. While we have no control over what information third party websites put into their URLs or where they put it, we make every commercially viable effort to purge our databases of any personally identifiable information. The data collection software uses a proprietary rules engine to search through all URLs, before transmitting them to its database, to strip out any such personally identifiable information. We do not disclose the contents of individual URLs stored in our databases so we will not release or use this information. Further, we aggregate data on hundreds of thousands of users before supplying data to our clients, thereby ensuring that an individual's privacy remains intact at all times.
>
> *See* Consumer Input Privacy Policy, Exhibit 6.
>
> In addition, the data collection software uses a proprietary rules engine to search through all URLs, before transmitting them directly to its database, to strip out any such personally identifiable information, thus ensuring your privacy.
>
> *See* Consumer Input Panel, Frequently Asked Questions, Exhibit 7.

15. Compete used data filters to prevent the collection and use of some sensitive data. However, those filters were too narrow and improperly structured to avoid collecting such data. For instance, a filter was designed to prevent the collection of personal identification numbers for financial accounts, and would have prevented collection of that data if a website used the field name "PIN." However, the filter would not have prevented such collection if a website used similar field names such as "personal ID" or "security code." In addition, Compete failed to implement a simple, commonly used, algorithm to screen out credit card numbers, and Compete filtered some types of information only after that information had been transmitted in clear text via the Internet to its servers.

**Compete's Data Security Practices**

16. In addition to the representations made about the collection of data, Compete made statements about the security of user data such as the following:

> We take reasonable security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of personal information. These measures include internal reviews of our data collection, storage and processing practices and security practices.

*See* General Compete Privacy Policy, Exhibit 5.

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

    a. created unnecessary risks of unauthorized access to consumer information by 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 design and implement reasonable information safeguards to control the risks to customer information; and

    c. failed to use readily available, low-cost measures to assess and address the risk that the data collection software would collect sensitive consumer information that it was not authorized to collect.

18. These security failures resulted in the creation of unnecessary risk to consumers' personal information. Compete transmitted the information it gathered – including sensitive information – over the Internet in clear readable text. Tools for capturing data in transit 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.

19. After flaws in Compete's data collection practices were revealed publicly in January 2010, Compete upgraded its filters, added new algorithms to screen out information such as credit card numbers, and began encrypting data in transit. The company stopped distributing the Compete Toolbar to new customers, and began to distribute its Consumer Input Panel software to new customers through third parties rather than directly. It continued to collect and use consumer data, however.

## VIOLATIONS OF THE FTC ACT

### Count 1

20. Through the means described in Paragraphs 7-9, respondent has represented, expressly or by implication, that its products would collect and transmit information about the websites consumers visited.

21. Respondent failed to disclose that its products would also collect and transmit much more extensive information about the Internet behavior that occurs on consumers' computers, and 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 act or practice.

**Count 2**

22. Through the means described in Paragraphs 13-14, respondent has represented, expressly or by implication, that it stripped all personal information out of the data it collected before transmitting it from consumers' computers.

23. In truth and in fact, Compete did not strip all personal information out of the data before transmitting it from consumers' computers. As described in Paragraph 15 the consumer-side filters were too narrow and improperly structured to effectively scrub personal data before transmission to Compete's servers. Therefore, the representation set forth in Paragraph 22 was, and is, false or misleading and constitutes a deceptive act or practice.

**Count 3**

24. Through the means described in Paragraph 16, respondent has represented, expressly or by implication, that it employs reasonable and appropriate measures to protect data obtained from consumers from unauthorized access.

25. In truth and in fact, as described in Paragraphs 10-11, 15 and 17-18, respondent did not implement reasonable and appropriate measures to protect data obtained from consumers from unauthorized access. Therefore, the representation set forth in Paragraph 24 was, and is, false or misleading and constitutes a deceptive act or practice.

**Count 4**

26. As described in Paragraphs 10-12, 15 and 17-18, 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 was not offset by countervailing benefits to consumers or competition and was not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

27. 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 twentieth day of February, 2013, has issued this complaint against respondent.

By the Commission, Chairman Leibowitz and Commissioner Wright not participating.

Donald S. Clark
Secretary

SEAL