UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of ZANGO, INC. f/k/a 180SOLUTIONS, INC., a corporation, KEITH SMITH, individually and as an officer of the corporation, and DANIEL TODD, individually and as an officer of the corporation.	FILE NO. 052 3130 DOCKET NO. _____

COMPLAINT

The Federal Trade Commission, having reason to believe that Zango, Inc. f/k/a 180solutions, Inc., a corporation, Keith Smith, individually and as an officer of the corporation, and Daniel Todd, individually and as an officer of the corporation (collectively "Respondents"), have 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 Zango, Inc. f/k/a 180solutions, Inc., is a Washington corporation with its principal place of business located at 3600 136th Place SE, Bellevue, Washington 98006. On June 7, 2006, 180solutions merged with New York-based Hotbar, Inc. and changed the combined company's name to Zango, Inc.

2. Respondent Keith Smith is a founder and officer of the corporate respondent. Individually or in concert with others, he formulates, directs, controls, or participates in the policies, acts, or practices of the corporation, including the acts and practices alleged in this complaint. His principal office or place of business is the same as that of Zango, Inc.

3. Respondent Daniel Todd is a founder and officer of the corporate respondent. Individually or in concert with others, he formulates, directs, controls, or participates in the policies, acts, or practices of the corporation, including the acts and practices alleged in this complaint. His principal office or place of business is the same as that of Zango, Inc.

4. The acts and practices of Respondents alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

5. Since at least 2002, Respondents have developed advertising software programs

("adware"), including without limitation programs called n-CASE, 180Search Assistant, Zango, and Seekmo, and distributed such programs to consumers' computers via Internet downloads.

6. When installed on a consumer's computer, Respondents' adware monitors Internet use on the computer and displays pop-up advertisements based on that Internet use. Consumers have received over 6.9 billion pop-up advertisements as a result of Respondents' adware.

7. Respondents' adware has been installed on U.S. consumers' computers over 70 million times.

8. One of Respondents' primary methods of distributing their adware is or has been to pay third-party affiliates to install Respondents' adware on consumers' computers.

9. Respondents know or have known that their affiliates retained numerous third-party sub-affiliates to install Respondents' adware on consumers' computers.

10. In numerous instances, Respondents, through affiliates and sub-affiliates acting on behalf and for the benefit of Respondents, bundled Respondents' adware with purportedly free software programs (hereinafter "lureware"), including without limitation Internet browser upgrades, utilities, screen savers, games, peer-to-peer file sharing, and/or entertainment content. Respondents, through affiliates and sub-affiliates, generally represented the lureware as being free.

11. When installing the lureware, consumers often have been unaware that Respondents' adware would also be installed because that fact was not adequately disclosed to them. In some instances, no reference to Respondents' adware was made on the website offering the lureware or in the install windows. In other instances, information regarding Respondents' adware was available only by clicking on inconspicuous hyperlinks contained in the install windows or in lengthy terms and conditions regarding the lureware. Because the lureware often was bundled with several different programs, the existence and information about the effects of Respondents' adware could only be ascertained, if at all, by clicking through multiple inconspicuous hyperlinks.

12. In numerous other instances, Respondents, through affiliates and sub-affiliates acting on behalf and for the benefit of Respondents, have installed Respondents' adware on consumers' computers by exploiting security vulnerabilities in Internet web browsers. Installations by this process, also known as "drive-by" downloads or "stealth" installations, provided no notice to consumers that Respondents' adware was being installed on their computers.

13. Respondents knew or should have known that there was widespread failure by their affiliates and sub-affiliates to provide adequate notice of their adware and obtain consumer consent to its installation. Indeed, notwithstanding their own contractual provisions or codes of conduct to the contrary, Respondents continued to allow certain affiliates, who were providing a

large volume of installations, to install Respondents' adware for as long as seventeen months after Respondents became aware of the unauthorized installations.

14. Until at least mid-2005, Respondents made identifying, locating, and removing their adware extremely difficult for consumers by, in numerous instances, among other practices:

a. Failing to identify adequately the name or source of the adware in pop-up ads so as to enable consumers to locate the adware on their computers;

b. Naming adware files or processes with names resembling core systems software or applications and placing files in a variety of locations;

c. Listing the adware in the Windows Add/Remove utility under names, including "Uninstall 180search Assistant," intended and/or likely to confuse the consumer (*i.e.*, the consumer would not want to remove a program needed to uninstall the adware);

d. Requiring consumers to follow a multiple-step procedure to uninstall the adware, including having a live connection to the Internet and downloading additional software from Respondents;

e. Requiring consumers who sought to uninstall the adware to click through multiple warning messages;

f. Representing to consumers that the adware did not show pop-up ads, that uninstalling the adware would not prevent the consumer from getting pop-up ads, and/or by exaggerating the consequences of uninstalling the adware;

g. Failing to disclose adequately that, in some versions of the adware, disabling the display of Respondents' pop-up advertisements would not disable the adware from monitoring and generating logs of the Internet browsing activities of consumers using that machine nor disable Respondents' collection of such information;

h. Providing an uninstall tool that failed to uninstall the adware in whole or part;

i. Installing technology on consumers' computers to silently reinstall the adware when consumers have attempted to remove it manually or to remove it using third-party anti-spyware or anti-adware

programs; and/or

j. Reinstalling the adware files on the consumer's computer with randomly generated names to avoid further detection and removal.

15. Respondents' practices forced consumers to invest significant time and effort, often including the expense of purchasing third party anti-spyware applications, to detect and rid their computers of Respondents' unwanted adware.

VIOLATIONS OF THE FTC ACT

Deceptive Failure Adequately to Disclose Adware

16. In numerous instances, as described in Paragraphs 8 through 11, Respondents, through affiliates and sub-affiliates acting on behalf and for the benefit of Respondents, represented to consumers, expressly or by implication, that they would receive lureware (including without limitation Internet browser upgrades, utilities, screen savers, games, peer-to-peer file sharing, and/or entertainment content). In numerous instances, Respondents, through affiliates and sub-affiliates acting on behalf and for the benefit of Respondents, failed to disclose, or failed to disclose adequately, that the lureware was bundled with Respondents' adware that would monitor consumers' Internet use and cause consumers to receive numerous pop-up advertisements based on such use. The bundling of adware would be material to consumers in their decision whether to install the lureware. The failure adequately to disclose this fact, in light of the representations made, was, and is, a deceptive act or practice.

Unfair Installation of Adware

17. In numerous instances, as described in Paragraphs 8 through 15, Respondents, through affiliates and sub-affiliates acting on behalf of and for the benefit of Respondents, installed on consumers' computers, without their knowledge or authorization, adware that could not be reasonably identified, located, or removed by consumers. Consumers thus have had to spend substantial time and/or money to locate and remove this adware from their computers. Respondents' practice has caused or is likely to cause substantial injury to consumers that cannot reasonably be avoided by the consumers themselves and is not outweighed by benefits to consumers or competition. These acts and practices were, and are, unfair.

Unfair Uninstall Practices

18. In numerous instances, as described in Paragraphs 14 through 15, Respondents failed to provide consumers with a reasonable and effective means to identify, locate, and remove Respondents' adware from their computers. Consumers thus have had to spend substantial time and/or money to locate and remove this adware from their computers. Respondents' practices have caused or are likely to cause substantial injury to consumers that cannot reasonably be

avoided by consumers themselves and is not outweighed by benefits to consumers or competition. These acts and practices were, and are, unfair.

19. The acts and practices 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, on this ____ day of _____, ____, issues this complaint against Respondents.

By the Commission.

Donald S. Clark
Secretary