062 3057

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of	)	
GUIDANCE SOFTWARE, INC.,	)	**DOCKET NO. C-4187**
a corporation.	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that Guidance Software, Inc. ("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 Guidance Software, Inc. is a California corporation with its principal office or place of business at 215 N. Marengo Ave., Pasadena, California, 91101.

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

3. Respondent sells software and related training, materials, and services that customers use to, among other things, investigate and respond to computer breaches and other security incidents. Through its Professional Services Division, respondent also performs forensic examinations of customer computer systems.

4. Respondent operates a computer network that it uses for routine corporate activities and that customers use, in conjunction with respondent's website (www.guidancesoftware.com) and web application program ("web application"), to obtain information and to buy respondent's products and services (hereinafter, "corporate network"). Respondent also operates a separate computer network that does not connect to the corporate network or the internet and is used only by its Professional Services Division.

5. In selling its products and services, respondent routinely collected sensitive personal information from customers, including name, address, email address, telephone number, and, for customers paying with a credit card, the card number, expiration date, and security code number. It collected this information through its website, sales representatives, and telephone and fax orders.

6. Respondent stored sensitive personal information obtained from customers on the corporate network on a computer accessible through its website.

7. Since at least 2002, respondent has disseminated or caused to be disseminated privacy policies and statements, including, but not necessarily limited to the following statements regarding the privacy and confidentiality of sensitive information collected from customers:

> **Security**
> This website takes every precaution to protect our users' information. When users submit sensitive information via the website, your information is protected both online and off-line. When our registration/order form asks users to enter sensitive information (such as credit card number and/or social security number), that information is encrypted and is protected with the best encryption software in the industry - SSL. While on a secure page, such as our order form, the lock icon on the bottom of Web browsers such as Netscape Navigator and Microsoft Internet Explorer becomes locked, as opposed to un-locked, or open, when you are just 'surfing'. . . . While we use SSL encryption to protect sensitive information online, we also do everything in our power to protect user-information off-line. . . . (Exhibit A, Guidance Software Privacy Statement accessible through respondent's corporate website, January 1, 2004 (emphasis in original)).
>
> Guidance Software is committed to keeping the data you provide us secure and will take reasonable precautions to protect your information from loss, misuse or alteration. (Exhibit B, Guidance Software Privacy Policy accessible through respondent's online store, July 19, 2003).

8. Until December 7, 2005 respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive personal information stored on its corporate network. In particular, although it employed SSL encryption, respondent: (1) stored the information in clear readable text; (2) did not adequately assess the vulnerability of its web application and network to certain commonly known or reasonably foreseeable attacks, such as "Structured Query Language" (or "SQL") injection attacks; (3) did not implement simple, low-cost, and readily available defenses to such attacks; (4) stored in clear readable text network user credentials that facilitate access to sensitive personal information on the network; (5) did not use readily available security measures to monitor and control connections from the network to the internet; and (6) failed to employ sufficient measures to detect unauthorized access to sensitive personal information.

9. Beginning in September 2005 and continuing through December 7, 2005, a hacker exploited the failures set forth in Paragraph 8 by using SQL injection attacks on

respondent's website and web application to install common hacking programs on respondent's corporate network. The hacking programs were used to find sensitive personal information, including credit card numbers, expiration dates, and security code numbers, stored on the corporate network and to transmit the information over the internet to computers outside the network. As a result, the hacker obtained unauthorized access to information for thousands of credit cards.

10. Respondent became aware of the breach in December 2005, at which time it took steps to prevent further unauthorized access, sent breach notification letters to customers for whom it had or could obtain addresses, and notified law enforcement.

11. Through the means described in Paragraph 7, respondent represented, expressly or by implication, that it implemented reasonable and appropriate measures to protect sensitive personal information it obtained from customers against unauthorized access.

12. In truth and in fact, respondent did not implement reasonable and appropriate measures to protect sensitive personal information it obtained from customers against unauthorized access. In particular, respondent failed to implement procedures that were reasonable and appropriate to: (1) detect reasonably foreseeable web application vulnerabilities, and (2) prevent attackers from exploiting such vulnerabilities and obtaining unauthorized access to sensitive personal information. Therefore, the representation set forth in Paragraph 7 was, and is, false or misleading.

13. The acts and practices of respondent as alleged in this complaint constitute 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 30th day of March 2007, has issued this complaint against Respondent.

By the Commission.

Donald S. Clark
Secretary