Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Guidance Software, Inc., File No. 062 3057

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Guidance Software Inc. ("Guidance").

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.

Guidance 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. In selling its products and services, Guidance 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 and stored the information on its computer network. This matter concerns alleged false or misleading representations Guidance made about the security it provided for this information.

The Commission's proposed complaint alleges that Guidance represented that it implemented reasonable and appropriate security measures to protect the privacy and confidentiality of personal information. The complaint alleges this representation was false because Guidance engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive personal information stored on its computer network. In particular, although it employed SSL encryption, Guidance: (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.

The complaint further alleges that beginning in September 2005 and continuing through December 7, 2005, a hacker exploited these vulnerabilities by using SQL injection attacks on Guidance's website and web application to install common hacking programs on Guidance's computer network. The hacking programs were used to find sensitive personal information, including credit card numbers, expiration dates, and security code numbers, stored on the 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.

The proposed order applies to personal information Guidance obtains from consumers. It contains provisions designed to prevent Guidance from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits Guidance, in connection with the online advertising, marketing, promotion, offering for sale, or sale of any product or service, from misrepresenting the extent to which it maintains and protects the privacy, confidentiality, or security of any personal information collected from or about consumers.

Part II of the proposed order requires Guidance to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to Guidance's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. Specifically, the order requires Guidance 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 customer information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the 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 retain service providers capable of appropriately safeguarding personal information they receive from Guidance, require service providers by contract to implement and maintain appropriate safeguards, and monitor their safeguarding of personal information.

- Evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that it knows or has reason to know may have material impact on its information security program.

Part III of the proposed order requires that Guidance obtain within 180 days, and on a biennial basis thereafter for a period of ten (10) 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

Part II of the proposed order; and (2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected.

Parts IV through VIII of the proposed order are reporting and compliance provisions. Part IV requires Guidance to retain documents relating to their 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, Guidance must retain the documents for a period of three years after the date that each assessment is prepared. Part V requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates that Guidance submit compliance reports to the FTC. Part VIII is a provision "sunsetting" the order 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 their terms in any way.