

Complaint

IN THE MATTER OF

GUIDANCE SOFTWARE, INC.CONSENT ORDER, ETC. , IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT*Docket C-4187; File No. 062 3057**Complaint, March 30, 2007 — Decision, March 30, 2007*

This consent order addresses representations that respondent Guidance Software, Inc., made as to the security of the sensitive personal information it collected from customers and its failure to actually safeguard the information. Guidance failed to provide reasonable and appropriate security for sensitive personal information stored on its computer network, and in 2005, a hacker exploited vulnerabilities in the respondent's website to obtain unauthorized access to information for thousands of credit cards. The order prohibits Guidance from misrepresenting the extent to which it maintains and protects the privacy, confidentiality, or security of any personal information collected from or about consumers. The order requires Guidance to establish and maintain a comprehensive information security program to protect the security, confidentiality, and integrity of such information. In addition, the respondent is required to obtain biennial assessments of its security program from a qualified, objective, independent third-party professional. The order also includes certain reporting and compliance provisions.

Participants

For the *Commission*: Katrina A. Blodgett, Kathryn D. Ratté,
and Alain Sheer.

For the *Respondents*: Elaine Kolish and Marc Zwillinger,
Sonnenschein Nath & Rosenthal, LLP.

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

Complaint

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, Acorporate 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.

Complaint

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 unlocked, 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

Complaint

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

Complaint

sensitive personal information it obtained from customers against unauthorized access.

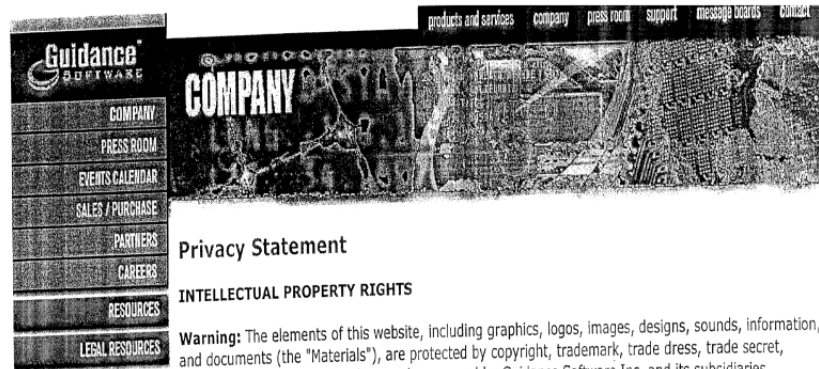
12. In truth and in fact, respondent did not implement reasonable and appropriate measures to protect sensitive personal information it obtained from customers against unauthorized access. In particular, respondent failed to implement procedures that were reasonable and appropriate to: (1) detect reasonably 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 thirtieth day of March, 2007, has issued this complaint against Respondent.

By the Commission.

Complaint Exhibits

Exhibit A**Privacy Statement****INTELLECTUAL PROPERTY RIGHTS**

Warning: The elements of this website, including graphics, logos, images, designs, sounds, information, and documents (the "Materials"), are protected by copyright, trademark, trade dress, trade secret, unfair competition and other laws and are owned by Guidance Software Inc. and its subsidiaries, divisions and affiliates ("Guidance Software"); or its suppliers, vendors or other third parties who have contributed Materials to the website (each a "Supplier"). In no event shall any of the Materials be copied, reproduced, distributed, displayed, downloaded, stored in a retrieval system, or transmitted in any form without the prior express written permission of Guidance Software and/or its Supplier. EnCase®, the EnCase logo, EnScript™ and other Guidance Software products and brands mentioned in this website are registered trademarks or trademarks of Guidance Software in the United States and/or other countries. The names of actual products and companies mentioned in this website may be registered trademarks or trademarks of their respective owners. Any rights not expressly granted herein are reserved.

General Disclaimer

THE MATERIALS ON THIS WEBSITE COULD INCLUDE INACCURACIES OR TYPOGRAPHICAL ERRORS AND ARE SUBJECT TO CHANGE AT ANY TIME. THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, GUIDANCE SOFTWARE AND ITS SUPPLIERS HEREBY DISCLAIM ALL WARRANTIES, EITHER EXPRESSED OR IMPLIED, AND CONDITIONS WITH RESPECT TO THE MATERIALS, THEIR QUALITY, PERFORMANCE, SUITABILITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

Links to Other Websites

As a convenience to you, this website may contain links to websites controlled by parties other than Guidance Software. Guidance Software is not responsible for and does not endorse the privacy practices or content of these third party websites.

Limitation of Liability

IN NO EVENT WILL GUIDANCE SOFTWARE AND ITS SUPPLIERS BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT OR TORT, ARISING OUT OF THE USE OR INABILITY TO USE THE MATERIALS AVAILABLE ON THIS WEBSITE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, AND WITHOUT LIMITATION, GUIDANCE SOFTWARE SHALL HAVE NO LIABILITY FOR ANY LOSS OF USE, DATA, INCLUDING THE COSTS OF RECOVERING SUCH DATA, OR PROFITS.

Complaint Exhibits

Privacy Statement

Guidance Software has created this privacy statement in order to demonstrate our firm commitment to your privacy. We intend to give you as much control as possible over your personal information (individually identifiable information about an individual collected online) and strive to help you protect your privacy while using our services. The purpose of our policy is to inform you about the types of information we gather about you when you visit our site, how we may use that information, whether we disclose it to anyone. Please read this notice. By using this site, you signify your assent to our privacy policy. If you do not agree to this policy, please do not use our sites. The following discloses our information gathering and dissemination practices for this website: www.guidancesoftware.com

Information Collection and Use

Guidance Software is the sole owner of the information collected on this site. We will not sell, share, or rent this information to others. Guidance Software collects information from our users at several different points on our website.

Registration

In order to use some portions of this website, a user must first complete the registration form. During registration a user is required to give their contact information (such as name and email address). This information is used to contact the user about the products and services offered by Guidance Software.

Order Information

We request information from the user on our order form. Here a user must provide contact information (like name and shipping address) and financial information (like credit card number, expiration date). This information is used for billing purposes and to fill customer's orders. If we have trouble processing an order, this information is used to contact the user.

Cookies

A cookie is a piece of data stored on the user's hard drive containing information about the user. Usage of a cookie is in no way linked to any personally identifiable information while on our site. Once the user closes their browser, the cookie simply terminates. For instance, by setting a cookie on our site, the user would not have to log in a password more than once, thereby saving time while on our site. If a user rejects the cookie, they may still use our site. Cookies can also enable us to track and target the interests of our users to enhance the experience on our site.

Public Forums

This site makes chat rooms, forums, mailing lists, message boards, and/or news newsgroups available to its users. Please remember that any information that is disclosed in these areas becomes public information and you should exercise caution when deciding to disclose your personal information.

Log Files

We use IP addresses to analyze trends, administer the site, track user's movement, and gather broad demographic information for aggregate use. IP addresses are not linked to personally identifiable information.

Links

This web site contains links to other sites. Please be aware that we are not responsible for the privacy practices of such other sites. We encourage our users to be aware when they leave our site and to read

Complaint Exhibits

the privacy statements of each and every web site that collects personally identifiable information. This privacy statement applies solely to information collected by this Web site.

Newsletter

If a user wishes to subscribe to our legal newsletter, we ask for contact information such as name and email address.

Surveys & Contests

From time-to-time our site requests information from users via surveys or contests. Participation in these surveys or contests is completely voluntary and the user therefore has a choice whether or not to disclose this information. Information requested may include contact information (such as name and shipping address), and demographic information (such as zip code, age level). Contact information will be used to notify the winners and award prizes. Survey information will be used for purposes of monitoring or improving the use and satisfaction of this site.

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'. To learn more about SSL, follow this link. While we use SSL encryption to protect sensitive information online, we also do everything in our power to protect user-information off-line. All of our users' information, not just the sensitive information mentioned above, is restricted in our offices. Only employees who need the information to perform a specific job (for example, our billing clerk or a customer service representative) are granted access to personally identifiable information. Furthermore, ALL employees are kept up-to-date on our security and privacy practices. Any time new policies are added, our employees are notified and/or reminded about the importance we place on privacy, and what they can do to ensure our customers' information is protected. Finally, the servers that we store personally identifiable information on are kept in a secure environment, behind a locked cage. If you have any questions about the security at our website, you can send an email to our [webmaster](#).

Software and Training Updates

We also send the user product and service announcement updates. We communicate with the user to provide requested services and information via email.

Notification of Changes

If we decide to change our privacy policy, we will post those changes on our Homepage so our users are always aware of what information we collect, how we use it, and under circumstances, if any, we disclose it. If at any point we decide to use personally identifiable information in a manner different from that stated at the time it was collected, we will notify users by way of an email. Users will have a choice as to whether or not we use their information in this different manner. We will use information in accordance with the privacy policy under which the information was collected.

Complaint Exhibits

Exhibit B

GUIDANCE SOFTWARE PRIVACY POLICY

Guidance Software respects your privacy. We use your information to support and enhance our relationship with you; for example, to process your purchase, provide service and support, and share product, service and company news and offerings with you. We do not sell your personal information. We only share your personal data for marketing purposes outside Guidance Software with your consent, as required by law or to protect Guidance Software, its customers, or the public, or with companies that help Guidance Software fulfill its obligations with you (such as shipping companies). At any time you may contact Guidance Software with any privacy questions or concerns you may have. You also may ask at any time to see the data you have given us and request correction or deletion. We strive to ensure a high level of security and confidentiality.

We've developed our privacy policy from industry guidelines and standards, and local, national, and international laws and requirements. All privacy practices and methods described in this policy apply only insofar as permitted by the applicable standards, laws and requirements.

Thanks again for placing your trust in Guidance Software.

INFORMATION COLLECTED

During the sales process, or through trade shows, marketing events, and other activities, Guidance Software may collect information from you. For example, we request information from you when you:

1. Register on www.guidancesoftware.com
2. Request a demo disk
3. Request a quotation or information
4. Register for a webinar, seminar, or other informational event
5. Place an order
6. Participate in a sweepstakes or other promotional offer
7. Subscribe to a newsletter or a mailing list
8. Request assistance from Guidance Software

We may ask you for your name, address, e-mail address, type of business, and credit card information, as well as other similar personal information.

HOW WE USE YOUR INFORMATION

The information you provide will be used to support your relationship with Guidance Software. Among other things, your information may be used to alert you to product upgrades or special offers, and to market or sell Guidance Software products or services to you. Your information may be combined with information collected about you by Guidance Software or third parties, with information that is collected about you from public records, or with information that Guidance Software may acquire from third parties.

DATA SHARING AND TRANSFER

Information regarding you (such as name, address and phone number) or your order and the products you purchase will not be given or sold to any outside organization for its use in marketing or solicitation without your consent. In addition, occasionally Guidance Software will share contact information, such as name and address, with third parties with whom we have partnered to provide specific services to Guidance Software, or services on behalf of Guidance Software.

In addition, Guidance Software may be required to disclose your information in connection with law enforcement, fraud prevention, regulation, and other legal action or if Guidance Software reasonably believes it is necessary to do so to protect Guidance Software, its customers, or the public.

Complaint Exhibits

Guidance Software is an expanding business, and like other companies, we sometimes acquire or divest business units. As part of such transfers, we may convey the business assets of the particular business unit, including information that you have supplied.

DATA SECURITY AND RESPONSIBILITY

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. Vendors, contractors, or partners of Guidance Software who have access to your information in connection with providing services for Guidance Software are required to keep the information confidential and are not permitted to use this information for any other purpose than to carry out the services they are performing for Guidance Software.

Your information will generally be stored in our Guidance Software databases, which are located in the United States. For easier processing of e-mail communications, or other marketing purposes, however, your information may be sent, usually on a temporary basis, to countries outside the United States. Guidance Software data protection standards are the same, regardless of where your information is stored.

YOU CAN OPT-OUT OF RECEIVING FURTHER MARKETING FROM GUIDANCE SOFTWARE

Periodically, we may send you information about our various products and services, or other products and services we feel may be of interest to you. If you do not want to receive such information, simply contact us at the address set forth below.

OTHER SITES

Guidance Software is not responsible for the privacy practices or the content of other Websites. We recommend that you carefully read the privacy policies of each site you visit.

CONTACT US

Please send us your questions or comments regarding our Privacy Policy or your information to:

Privacy Compliance Coordinator
Guidance Software, Inc.
P.O. Box _____
Pasadena, CA 91101
USA
privacy@guidancesoftware.com

Guidance Software will be happy to respond to your questions and comments.

YOUR ACCEPTANCE OF OUR PRIVACY PRACTICES

By using the Guidance Software website, purchasing from Guidance Software, or participating in a Guidance Software service or program, you signify your acceptance of the terms and conditions of this Privacy Policy. Guidance Software may make changes to this Privacy Policy from time to time. We will post changes to our Privacy Policy on the Guidance Software website, so from time to time please check the Privacy Policy posted there.

Last updated: 7/19/03

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 Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq*;

The Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondent that the law has been violated as alleged in such Complaint, or that 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 has reason to believe that the Respondent has violated the said Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure described in Section 2.34 of its Rules, the Commission hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:

1. Proposed respondent Guidance Software, Inc. is a California corporation with its principal office or place of business at 215 N. Marengo Avenue, Pasadena, California, 91101.

Decision and Order

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

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

1. “Personal information” shall mean individually identifiable information from or about a 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 email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals a consumer’s email address; (d) a telephone number; (e) a Social Security number; (f) credit or debit card information, including card number, expiration date, and numerical security code; (g) 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 a consumer; or (h) any other information from or about a consumer that is combined with (a) through (g) above.

2. Unless otherwise specified, “respondent” shall mean Guidance Software, Inc. and its successors and assigns, officers, agents, representatives, and employees.

3. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the online advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce,

Decision and Order

shall not misrepresent in any manner, expressly or by implication, the extent to which respondent maintains and protects the privacy, confidentiality, security, or integrity of any personal information collected from or about consumers.

II.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. 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, 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 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 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)

Decision and Order

prevention, detection, and response to attacks, intrusions, 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 effectiveness of the safeguards' key controls, systems, and procedures.

D. the development and use of reasonable steps to retain service providers capable of appropriately safeguarding personal information they receive from respondent, requiring service providers by contract to implement and maintain appropriate safeguards, and monitoring their safeguarding of personal information.

E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subparagraph 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.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Paragraph II of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession. 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 ten (10) 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, 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 Paragraph II 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 by 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.

Respondent shall provide the initial Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relied upon to prepare such 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

Decision and Order

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.

IV.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and

B. for a period of three (3) years after the date of preparation of each biennial Assessment required under Paragraph III of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relating to respondent's compliance with Paragraphs II and III of this order for the compliance period covered by such biennial Assessment.

V.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

Decision and Order

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation 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 corporation; the creation or dissolution of a subsidiary, 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 either corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation 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. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VII.

IT IS FURTHER ORDERED that respondent shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VIII.

This order will terminate on March 30, 2027, or twenty (20) years from the most recent date that the United States or the Federal Trade 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:

Analysis to Aid Public Comment

- A. any Paragraph in 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 Paragraph.

Provided, further, that if such complaint is dismissed or a federal court rules that 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 Paragraph as though the complaint had never been filed, except that the 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 OF PROPOSED CONSENT ORDER
TO AID PUBLIC COMMENT**

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.

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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.

Analysis to Aid Public Comment

- 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.

Analysis to Aid Public Comment

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 "Asunsetting" 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.

Complaint

IN THE MATTER OF

**THE BOEING COMPANY AND LOCKHEED
MARTIN CORPORATION**

CONSENT ORDER, ETC. , IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 7 OF THE CLAYTON ACT AND SEC. 5 OF THE FEDERAL TRADE
COMMISSION ACT

Docket C-4188; File No. 051 0165
Complaint, May 1, 2007 — Decision, May 1, 2007

The purpose of this consent order is to remedy the anticompetitive effects resulting from the formation of United Launch Alliance L.L.C., a joint venture of the Boeing Company and Lockheed Martin Corporation that will provide space launch services to the Department of Defense and other U.S. government customers. The U.S. Department of Defense informed the Commission that the creation of United Launch Alliance will advance U.S. national security interests by improving the United States' ability to access space reliably, with the increase in reliability as an efficiency flowing from the joint venture. However, the Department had concerns about effects not related to national security benefits, anticompetitive effects of substantially lessening competition in the U.S. government markets for medium-to-heavy launch services and space vehicles. The order requires that United Launch Alliance cooperate on equivalent terms with all providers of government space vehicles; that the space vehicle businesses of Boeing and Lockheed provide equal consideration and support to all launch services providers when seeking any U.S. government delivery-in-orbit contract; and that Boeing, Lockheed, and United Launch Alliance safeguard competitively sensitive information obtained from other providers of space vehicles and launch services. To ensure compliance, Boeing and Lockheed must create selection criteria and have those criteria approved by the compliance officer, who will be appointed by the Secretary of Defense. Further, the order prohibits Boeing and Lockheed from selecting United Launch Alliance as a launch services supplier without the prior approval of the compliance officer. In addition, United Launch Alliance facilities must be physically separate from those of Boeing and Lockheed, and employees must be able to access only the facilities of their respective employer.