022 3260

UNITED STATES OF AMERICA

consumers must provide personal information, including, but not limited to, name, address, and credit or debit card number and expiration date. Respondents store this information in particular locations (called “tables”) within databases that support or connect to the website. For example, the credit card numbers received from purchasers on the website are stored in a single database table. Respondents also store product information, such as the sizes and colors in which a shirt is available, in other tables contained within the same databases.

5. Like most e-commerce websites, visitors interact with Respondents' website using a software program called an "application." Respondents' application was designed so that a visitor could use it to obtain product information from certain database tables, as well as to supply transaction information that was then stored in other tables in the databases. To facilitate communications between the website and a visitor, the application was designed to automatically present in clear readable text any information retrieved from or supplied to the databases.

6. Since June 1998, Respondents have disseminated or caused to be disseminated privacy policies on

www.guess.com, including but not necessarily limited to that attached as Exhibit B, containing the following statements:

> **Q: What is the Information Security Policy for GUESS? Online?**
> **A:** Providing a safe and secure environment for your order information is our top priority. Taking advantage of Secure Sockets Layer (SSL) technology, GUESS? ensures the security of your online transaction. The GUESS? Online Store is powered by Microsoft and Verisign and uses Cybersource SSL technology - the industry standard for encryption technology to create a secure transaction environment for commerce on the Internet. SSL technology encrypts files allowing only GUESS? to decode your information.

Exhibit B: About Guess?, http://www.guess.com/section.asp?section=help (emphasis in original).

8. Since at least October 2000, Respondents' application and website have been vulnerable to commonly known or reasonably foreseeable attacks from third parties attempting to obtain access to customer information stored in Respondents' databases. These attacks include, but are not limited to, web-based application attacks such as "Structured Query Language" ("SQL") injection attacks. Such attacks occur when an attacker enters certain characters in the address (or URL) bar of a standard web browser to direct the application to obtain information from the databases that support or connect to the website. Through such an attack, the application could be manipulated to gain access, in clear text, to every table in the www.guess.com databases, including the tables containing the credit card information supplied by purchasers.

9. Respondents created these vulnerabilities by failing to implement reasonable and appropriate measures to secure and protect the databases that support or connect to the website. Among other things, Respondents failed to: adopt policies and procedures adequate to protect sensitive consumer information collected though the website; test or otherwise assess the website's or the application's vulnerability to attacks; and implement reasonable measures to prevent website visitors from gaining access to database tables containing sensitive personal information about other consumers.

10. The risk of web-based application attacks is commonly known in the information technology industry, as are simple, publicly available measures to prevent such attacks. Security experts have been warning the industry about these vulnerabilities since at least 1997; in 1998, at least one security organization developed, and made available to the public at no charge, security measures which could prevent such attacks; and in 2000, the industry began receiving reports of

12. Through the means described in Paragraphs 6 and 7, Respondents have represented, expressly or by implication, that the personal information they obtained from consumers through www.guess.com was stored in an unreadable, encrypted format at all times.

13. In truth and in fact, the personal information Respondents obtained from consumers through www.guess.com was not stored in an unreadable, encrypted format at all times. Using a standard web browser, a commonly known attack could be employed to manipulate the web application and gain access, in clear readable text, to sensitive personal information about other consumers, including but not limited to, consumer names and credit card numbers and expiration dates. Therefore, the representation set forth in Paragraph 12 was false or misleading.

14. Through the means described in Paragraphs 6 and 7, Respondents have represented, expressly or by implication, that they implemented reasonable and appropriate measures to protect the personal information they obtained from consumers through www.guess.com against loss, misuse, or alteration.

15. In truth and in fact, Respondents did not implement reasonable and appropriate measures to protect the personal information they obtained from consumers through www.guess.com against loss, misuse, or alteration. In particular, Respondents failed to implement procedures that were reasonable and appropriate to: (1) detect reasonably foreseeable vulnerabilities of their website and application and (2) prevent visitors to the website from exploiting such vulnerabilities and gaining access to sensitive consumer data. Therefore, the representation set forth in Paragraph 14 was false or misleading.

16. The acts and practices of Respondents 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 thirtieth day of July, 2003, has issued this complaint against Respondents.

By the Commission.

Donald S. Clark
Secretary