0523094

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **William E. Kovacic, Chairman**
Pamela Jones Harbour
Jon Leibowitz
J. Thomas Rosch

In the Matter of	)	
REED ELSEVIER INC. and SEISINT, INC., corporations.	)	**DOCKET NO. C-4226**

COMPLAINT

The Federal Trade Commission, having reason to believe that Reed Elsevier Inc. and Seisint, Inc. 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 Reed Elsevier Inc. ("REI") is a Massachusetts corporation with its principal office or place of business at 125 Park Avenue, Suite 2300, New York, New York 10017. REI engaged in the acts and practices at issue in this complaint through LexisNexis, a division of REI with its principal office or place of business at 9333 Springboro Pike, Dayton, Ohio 45401.

2. Respondent Seisint, Inc. ("Seisint") is a Florida corporation with its principal office or place of business at 6601 Park of Commerce Boulevard, Boca Raton, Florida 33487.

3. Respondent REI acquired respondent Seisint on September 1, 2004, and since then has operated it as a wholly-owned subsidiary within LexisNexis. Respondent REI integrated respondent Seisint into LexisNexis by, among other things, using respondent Seisint's facilities, personnel, technologies, and products in LexisNexis' other business operations. Since the acquisition, respondent REI has controlled the acts and practices of respondent Seisint at issue in this complaint. Respondent Seisint is solely liable for its practices prior to the acquisition.

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

RESPONDENTS' BUSINESS PRACTICES

5. At all relevant times before and after the acquisition, respondents Seisint and REI have been in the business of collecting, maintaining, and selling information about consumers. Among other things, each respondent sells products that customers use to locate assets and people, authenticate identities, and verify credentials (collectively, "verification products").

6. Respondent Seisint sells verification products under its Accurint trade name (collectively, "Accurint verification products"). Accurint verification product customers include insurance companies, debt collectors, employers, landlords, law firms, and law enforcement and other government agencies. Respondent REI sells similar verification products, under various LexisNexis trade names.

7. In connection with their verification products, respondents:

   (a) collect and aggregate information about millions of consumers and businesses from public and nonpublic sources, including motor vehicle records and consumer identification information from credit reporting agencies, and maintain and store the information in computer databases.

   (b) operate computer networks and websites and provide software (such as web applications and search engines) through which a customer can use a verification product to search electronically for information in the respondent's computer databases. To conduct such a search, the customer enters a search term, such as a consumer's name, and retrieves through the search other items of information about the consumer.

   (c) charge customers a fee to search for and retrieve information from their databases.

8. Respondents' databases contain nonpublic and often highly sensitive personal information about consumers, including consumer identification information obtained from credit reporting agencies, such as Social Security numbers. It is widely recognized that misuse of such information -- and in particular consumers' Social Security numbers -- can facilitate identity theft and related consumer harms.

9. At all relevant times, respondents have implemented procedures to identify customers seeking access to their databases, limit access to nonpublic information to customers meeting certain criteria, and track searches their customers make. Such procedures include:

(a) steps to authenticate customers (or verify that the customers are who they claim to be) before permitting them to search the databases, usually by requiring each customer to log-in using a user ID and a password (collectively, "user credentials").

(b) rules governing the format of user credentials that customers must present for authentication.

(c) rules governing which customers can access nonpublic information and which are restricted to public information only.

(d) codes, assigned to each customer's user credentials, that permit the customer to access the types of information the customer is authorized to access.

Under these procedures, an unauthorized person logging-in with the user credentials of a legitimate verification product customer would be authenticated and could then access all of the information the legitimate customer could access, including sensitive nonpublic information if the customer were so authorized.

RESPONDENTS' SECURITY PRACTICES

10. Until at least mid-2005, respondents engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security to prevent unauthorized access to the sensitive consumer information stored in databases accessible using Accurint verification products ("Accurint databases"). In particular, respondents failed to establish or implement reasonable policies and procedures governing the creation and authentication of user credentials for authorized customers accessing Accurint databases. Among other things, respondents:

(a) failed to establish or enforce rules sufficient to make user credentials hard to guess. For example, respondents allowed Accurint customers to use the same word, including common dictionary words, as both the password and user ID, or a close variant of the user ID as the password;

(b) permitted the sharing of user credentials among a customer's multiple users, thus reducing likely detection of, and accountability for, unauthorized searches;

(c) failed to require periodic changes of user credentials, such as every 90 days, for customers with access to sensitive nonpublic information;

(d) failed to suspend user credentials after a certain number of unsuccessful log-in attempts;

(e) allowed customers to store their user credentials in a vulnerable format in cookies on their computers;

(f) failed to require customers to encrypt or otherwise protect credentials, search queries, and/or search results in transit between customer computers and respondents' websites;

(g) allowed customers to create new credentials without confirming that the new credentials were created by customers rather than identity thieves;

(h) did not adequately assess the vulnerability of the Accurint web application and computer network to commonly known or reasonably foreseeable attacks, such as "Cross-Site Scripting" attacks; and

(i) did not implement simple, low-cost, and readily available defenses to such attacks.

11. By the security practices set out in Paragraph 10, respondents established user ID and password structures that created an unreasonable risk of unauthorized access to sensitive consumer information stored in Accurint databases. Security professionals have issued public warnings about the security risk presented by weak user ID and password structures since the late 1990s, when well-publicized attacks to obtain customer passwords began to occur. Further, from attacks on user ID and password structures controlling access to Accurint databases, respondents have had notice of the risk since at least 2002. In addition, respondents did not use readily-available security measures to prevent or limit such attacks, such as by using well-known procedures that would limit or block attacks on user credentials. As a result of respondents' security practices, an attacker could easily guess or intercept the user credentials of legitimate customers and use them to gain access to sensitive information -- including Social Security numbers -- about millions of consumers.

12. On multiple occasions since January 2003, attackers exploited respondent Seisint's user ID and password structures to obtain without authorization the user credentials of legitimate Accurint customers. The attackers then used these credentials to make thousands of unauthorized searches for consumer information in Accurint databases. These attacks disclosed sensitive information about several hundred thousand consumers, including, in many instances, names, current and prior addresses, dates of birth, and Social Security numbers. Although some of these attacks occurred before respondent REI acquired respondent Seisint, they continued for at least 9 months after the acquisition, during which time respondent Seisint was operating under the control of respondent REI. Since March 2005, respondent REI through LexisNexis has notified over 316,000 consumers that the attacks disclosed sensitive information about them that could be used to conduct identity theft.

13. In a number of the incidents referred to in Paragraph 12, new credit accounts were opened in the names of consumers whose information was disclosed without authorization, and purchases were made on the new accounts. In other instances, identity thieves used sensitive information obtained without authorization from Accurint

databases to activate newly-issued credit cards stolen from legitimate cardholders, and then made fraudulent purchases on the cards. In response to such incidents, cards were cancelled and consumers holding them were unable to use them to access their credit and bank accounts until they received replacement cards. Further, because the incidents referred to in Paragraph 12 disclosed Social Security numbers and other sensitive information, several hundred thousand consumers face the possibility of future fraud.

VIOLATIONS OF THE FTC ACT

14. As set forth in Paragraphs 10 through 13, respondents failed to employ reasonable and appropriate measures to prevent unauthorized access to sensitive consumer information stored in Accurint databases. Respondents' practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

15. The acts and practices of respondents as alleged in this complaint constitute unfair 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 twenty-ninth day of July, 2008, has issued this complaint against respondents.

By the Commission.

Donald S. Clark
Secretary