0523094

A A A

A A

:

c c

c

)
)
)
)
)
)
)

A

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.

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.

(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