Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Reed Elsevier Inc. and Seisint, Inc., File No. 0523094

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Reed Elsevier Inc. ("REI") and Seisint, Inc. ("Seisint").

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.

The Commission's proposed complaint alleges that REI (through its LexisNexis division) and Seisint are data brokers. REI acquired Seisint on September 1, 2004 and has continued to operate Seisint under the Seisint name; REI also uses Seisint's technologies and facilities in REI's LexisNexis data broker business. In connection with Seisint's business, proposed respondents collect, and store in electronic databases, information about millions of consumers, including names, current and prior addresses, dates of birth, driver's license numbers, and Social Security numbers ("SSNs"). They also sell products customers use to retrieve information from the databases, including products to locate assets and people, authenticate identities, and verify credentials. Until at least mid-2005, access to information in Seisint databases was controlled using only user IDs and passwords ("credentials"). Seisint customers include insurance companies, debt collectors, employers, landlords, law firms, and law enforcement and other government agencies.

The complaint further alleges that REI and Seisint engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive consumer information stored in Seisint databases. In particular, they: (1) failed to make credentials hard to guess; (2) failed to require periodic changes of credentials (such as every 90 days, for customers with access to sensitive consumer information); (3) failed to suspend credentials after a certain number of unsuccessful log-in attempts; (4) allowed customers to store their credentials in a vulnerable format in cookies on their computers; (5) failed to require customers to encrypt or otherwise protect credentials, search queries, and/or search results in transit between customer computers and Seisint websites; (6) allowed customers to create new credentials without confirming that the new credentials were created by customers rather than identity thieves; (7) permitted users to share credentials; (8) did not adequately assess the vulnerability of Seisint's web application and computer network to commonly known or reasonably foreseeable attacks, such as "Cross-Site Scripting" attacks; and (9) did not implement simple, low-cost, and readily available defenses to such attacks. As a result, an attacker could easily guess or intercept the user credentials of legitimate customers and use them to access sensitive information -- including SSNs -- about millions of consumers.

The complaint alleges that on multiple occasions since January 2003, identity thieves exploited these vulnerabilities to obtain the credentials of legitimate Seisint customers. The thieves then used the credentials to make thousands of unauthorized searches for consumer information in Seisint databases. These breaches disclosed sensitive information about more than 300,000 consumers, including, in many instances, names, current and prior addresses, dates of birth, and SSNs. In some instances, the thieves opened new credit accounts in the names of consumers whose information was disclosed and made purchases on the new accounts. In other instances, they used the information to activate newly-issued credit cards stolen from legitimate cardholders and then made fraudulent purchases on the cards. Although some of these breaches occurred before REI acquired Seisint on September 1, 2004, they continued for at least 9 months after the acquisition, during which time Seisint was under REI's control.

The proposed order applies to nonpublic information sold by Seisint and LexisNexis, as well as by any other business within REI to the extent that the business sells products that include an SSN, driver's license number; date of birth; or bank, credit card, or other financial account number or information. The order also contains provisions designed to prevent respondents from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order requires each respondent to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of nonpublic personal information collected from or about consumers. The security programs must contain administrative, technical, and physical safeguards appropriate to the respondent'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 each respondent 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 select and retain service providers capable of appropriately safeguarding personal information they receive from the respondent, and require service providers by contract to implement and maintain appropriate safeguards.

- Evaluate and adjust its information security programs in light of the results of testing and monitoring, any material changes to 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 II of the proposed order requires each respondent to obtain within 180 days, and on a biennial basis thereafter for a period of twenty (20) 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 I 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 III through VII of the proposed order are reporting and compliance provisions. Part III requires respondents 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, respondents must retain the documents for a period of three years after the date that each assessment is prepared. Part IV requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part V ensures notification to the FTC of changes in corporate status. Part VI mandates that each respondent submit a compliance report to the FTC within 180 days, and periodically thereafter as requested. Part VII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

This is the Commission's nineteenth case to challenge the failure by a company to implement reasonable information security practices. Each of the Commission's cases to date has alleged that a number of security practices, taken together, failed to provide reasonable and appropriate security to prevent unauthorized access to consumers' information. The practices challenged in the cases have included, but are not limited to: (1) creating unnecessary risks to sensitive information by storing it on computer networks without a business need to do so; (2) storing sensitive information on networks in a vulnerable format; (3) failing to use readily available security measures to limit access to a computer network through wireless access points on the network; (4) failing to adequately assess the vulnerability of a web application and computer network to commonly known or reasonably foreseeable attacks; (5) failing to implement simple, low-cost, and readily available defenses to such attacks; and (6) failing to use readily available security measures to limit access between computers on a network and between such computers and the Internet. This proposed action against REI and Seisint is the first to challenge alleged security failures involving the security of passwords. Passwords are a critical part of a reasonable and appropriate security program because passwords are typically the first (and are often the only) method used to authenticate (or authorize) users to access resources, such as programs and databases, available on a computer network or online.

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 its terms in any way.