3/9/2005 *By Paul Roberts, IDG News Service MacCentral*

Hackers have compromised databases belonging to LexisNexis and stolen information on at least 32,000 people, according to a statement Wednesday from LexisNexis' parent company, Reed Elsevier PLC.

The hackers stole passwords, names, addresses, Social Security (news - web sites) and drivers license numbers of legitimate customers of the company's Seisint division. Seisint collects data on individuals that is used by law enforcement and private companies for debt recovery, fraud detection and other services.

LexisNexis identified the incidents in a review of security procedures and warned that there may be more incidents of data theft, Reed Elsevier said. The incident is eerily familiar to recent revelations about similar compromises at Seisint competitor ChoicePoint Inc., which acknowledged in February that hackers had access to data on 145,000 people.

Reed Elsevier did not immediately respond to requests for comment.

LexisNexis, which acquired Seisint Inc. of Boca Raton, Florida, in September for US $775 million, expressed regret for the incident and said it is notifying the individuals whose information may have been accessed and will provide them with credit monitoring services.

The company also said it notified law enforcement and is assisting with investigations of the fraudulent account access.

Like ChoicePoint, Seisint maintains a massive database of public and private information on individuals, including Social Security numbers, credit histories and criminal records. Seisint made the news in recent years as the data source behind the "Multistate Anti-Terrorism Information Exchange," or MATRIX, system, a program to bring together criminal and public records from participating U.S. states.

Bill Shrewsbury, a vice president at Seisint, said that identity thieves used a different approach to breach the company's database than what was used to get ChoicePoint's data, but declined to elaborate.

LexisNexis is taking actions to improve its ID and password administration security, and customer screening, the company said in its statement.

The incident is just the latest in a series of revelations about consumer data being leaked or lost. Those incidents include the ChoicePoint hack and Bank of America Corp.'s disclosure last week that it lost digital tapes containing the credit card account records of 1.2 million federal employees, including 60 U.S. senators.

ChoicePoint, of Alpharetta, Georgia, has also been the focus of intense scrutiny and criticism since it acknowledged that identity thieves posed as legitimate customers to gain access to the company's database of 19 billion public records. Some of the information stolen from ChoicePoint has since been used in about 750 identity theft scams, according to the company.

The company said last week that it is discontinuing data sales to many of its customers, except when that data helps complete a consumer transaction or helps government or law enforcement.

Since disclosing the security breach, ChoicePoint has been the subject of a U.S. Federal Trade Commission inquiry into its compliance with federal information security laws, a U.S. Securities

and Exchange Commission (news - web sites) (SEC) investigation into possible insider stock trading violations by its chief executive officer and chief operating officer and lawsuits alleging violations of the federal Fair Credit Reporting Act and California state law. ChoicePoint disclosed the inquiries in a filing to the SEC on March 4.