

# LexisNexis Security Breach Expands

By David Colker and John Spano, Times Staff Writers, Tuesday, April 12

The identity thieves who stole passwords to tap personal data from information broker LexisNexis hacked the records of more than 300,000 Americans, 10 times what the company first acknowledged, the company disclosed today.

The announcement today by London-based Reed Elsevier, which owns LexisNexis, indicates that security problems in the industry are more widespread than first thought.

The company said that it had uncovered 59 cases in which unauthorized persons "using IDs and passwords of legitimate customers" fraudulently acquired personal identifying data from its databases.

Reed Elsevier's director of corporate relations, Catherine May, emphasized that LexisNexis' infrastructure was not breached.

"This is about misuse of legitimate passwords and means of access," May said from London.

LexisNexis estimates that information on 310,000 U.S. individuals may have been accessed. When it first reported the thefts March 9, the company said about one-third of the victims were California residents.

LexisNexis said it will notify all individuals involved and is offering free credit bureau reports, credit monitoring for one year and fraud insurance. The company said it is cooperating with law enforcement authorities in an investigation of "potentially fraudulent misuse" of the data by hackers.

Reed Elsevier said the data stolen does not include "personal credit histories, medical records or financial records on individuals."

"The information concerned relates to names and addresses and other personal identifying information such as Social Security and driver's license numbers," Reed Elsevier said today.

Sen. Patrick J. Leahy (D-Vt.) of the Senate Banking Committee, at a hearing on identity theft last month, asked for an audit of security arrangements that the federal government has with databases run by LexisNexis and ChoicePoint, the other major data provider that was the victim of a mass infiltration by hackers this year. Several members of Congress have said they intend to introduce legislation calling for closer monitoring of information brokers by the Federal Trade Commission.

The company is investigating whether the fraud was carried out by people who posed as legitimate customers of the LexisNexis service or whether they gained access fraudulently.

"We don't know yet," said Steve Edwards, director of LexisNexis corporate communications. "We know they used legitimate customer logins and passwords."

Some of the unauthorized access in the ChoicePoint case involved legitimate customers. Edwards said his company conducts extensive screening of potential customers.

"We go through quite a bit of verification of customers. We determine the validity of business licenses. We do other types of background screening, such as checking memberships in professional associations and other credentials, such as previous news coverage," Edwards said.

LexisNexis customers with passwords include government agencies, law enforcement, banks and insurance companies, Edwards said.

ChoicePoint and LexisNexis compete in the booming business of providing personal data on millions of Americans to merchants, employers and government agencies.

Their services also are valuable to identity thieves who, posing as legitimate customers, use them to acquire Social Security numbers and other personal information to open fraudulent credit card accounts.

LexisNexis, a Dayton, Ohio-based company, is best known for its huge database of newspaper and magazine articles and case law.