The New York Times

TECHNOLOGY

Security Breach at LexisNexis Now Appears Larger

By HEATHER TIMMONS APRIL 13, 2005

LONDON, April 12 - Reed Elsevier, owner of the LexisNexis databases, said Tuesday that Social Security numbers, driver's license information and the addresses of 310,000 people may have been stolen, 10 times more than it originally reported last month.

The company said there were 59 separate instances in which unauthorized users "may have fraudulently acquired personal identifying information" through Seisint, a unit of LexisNexis. Seisint compiles information from government records and holds personal data about most American citizens. Its data is used by employers making hiring decisions, landlords choosing tenants and by debt collectors among others.

Unauthorized Seisint users often used log-in names and passwords that were assigned to legitimate customers, the chief executive of the LexisNexis Group, Kurt Sanford, said in an interview. LexisNexis found that the thieves were using the log-in names assigned to former employees of Seisint customers or were correctly guessing uncomplicated ID and password combinations or accessing customers' systems through a virus, Mr. Sanford said.

The announcement, along with reports earlier this year from ChoicePoint, another data broker, and Bank of America that personal information may have been stolen, added fuel to calls to regulate the $5 billion-a-year data-brokering industry. The Senate Judiciary Committee is currently holding hearings about the protection of personal data.

"This shows how we don't have a handle on how large and pervasive a problem identity theft really is," Senator Charles E. Schumer, Democrat of New York, said in an e-mail message. "When a company like LexisNexis so badly underestimates its own ID theft breaches, it is clear that things are totally out of hand."

Senator Schumer and Senator Bill Nelson, Democrat of Florida, said they were introducing a bill in Congress calling for a ban on the sale of Social Security numbers and for tighter controls for companies like ChoicePoint and Seisint. Several other pieces of legislation have been introduced over the last three months aimed at protecting consumer privacy and regulating data brokers.

Not surprisingly, data brokering executives, including Mr. Sanford, oppose some of the legislation, particularly the ban on the sale of Social Security numbers.

"No matter how perfect security is, it's not going to stop identity theft in the United States," because of the amount of information that is already available on the Internet and in public databases, Mr. Sanford said. Instead, he said, more steps should be taken to control how credit is granted, particularly the way that credit cards are used and issued.

Reed Elsevier, a publisher based in London, said it would notify all 310,000 individuals affected, and offer free fraud insurance and credit bureau reports for a year. It is also trying to improve its password system. LexisNexis began investigating security at Seisint in February, after customers complained about unexpectedly high monthly bills. Those bills were generated by unauthorized use of the customers' accounts.

Reed Elsevier said the announcement would have no immediate impact on its bottom line. But its share price fell 1.03 percent on Tuesday, closing at 530 pence in London. No similar problems have occurred in Europe because European Union regulations do not allow companies to buy and sell an individual's personal data.

American security experts contend that the Reed Elsevier announcement will be followed by others. "This is just the tip of the iceberg," said Stanton S. Gatewood, the University of Georgia's chief information security officer and a lecturer on the issue of data security.

"For so long, we've depended on companies like LexisNexis, and the government, to secure our information," Mr. Gatewood said. "But I'm here to tell you they're no more secure than anything else."

On March 9, Reed Elsevier gave the first sign there was a security problem with Seisint, which it purchased for $775 million in July 2004. The company said then that data from 32,000 individuals may have been fraudulently obtained, and that it would contact them by letter.

So far, 2 percent of the individuals contacted have responded, Reed said, and none of those have experienced any form of identity theft.

Tom Zeller Jr. contributed reporting for this article.
