

March 10, 2005

Another Data Broker Reports a Breach

By **TOM ZELLER Jr.****BUSINESS & LABOR**EXHIBIT NO. 6
DATE 3/22/05
BILL NO. HB 732

The LexisNexis Group, a major compiler of legal and consumer information, said yesterday that information on about 30,000 people - including names, addresses and Social Security numbers - may have fallen into the hands of thieves.

The announcement follows the recent disclosure of several other cases involving the loss or theft of consumer data. ChoicePoint, another major data broker, said last month that it had inadvertently sold the records of about 145,000 individuals to criminals. And the Bank of America said more recently that backup computer tapes containing information on more than a million of its customers had been lost.

The Federal Bureau of Investigation and the Treasury Department are investigating the LexisNexis incident, people close to the inquiry said. The concern in such cases is that criminals could use the information to open credit card accounts under the stolen names or engage in other forms of so-called identity theft.

LexisNexis said it had not yet determined how access might have been gained to the files but that it appeared to have involved unauthorized use of passwords of legitimate subscribers to its databases, rather than a hacker attack on its system.

The LexisNexis breach is almost certain to accelerate calls from privacy advocates and state and federal officials for greater scrutiny of the companies that buy, store and sell consumer data. The issue will be taken up today in a hearing before the Senate Banking, Housing and Urban Affairs Committee, and next Tuesday at a similar hearing before the House Energy and Commerce Committee.

"I personally see no socially redeeming value in anyone having the right to give away and sell my personal information unless I approve it," the chairman of the House Energy and Commerce Committee, Joe Barton, said yesterday. "Under current law these companies have a legal right to package it and do almost anything they want to do with it," Mr. Barton, Republican of Texas, said. "I just think that's fundamentally wrong. And in the Internet age, it's dangerous."

Some lawmakers expressed similar sentiments.

"We need to think proactively and treat these data troves with the same level of care and protection that we would any other valuables," a Senate Democrat, Patrick Leahy of Vermont, wrote in an e-mail statement. On behalf of the Senate Judiciary Committee, Mr. Leahy is scheduled to testify before the Senate banking committee hearing this afternoon. "Our peace of mind, our economy and even our nation's security depend on it," he wrote. The Judiciary Committee also plans to conduct hearings on the issue soon.

The industry is currently governed by a hodgepodge of state and federal laws. Critics have argued that

because those laws are ill-defined and often at odds, companies like ChoicePoint and LexisNexis are permitted to police themselves as they market consumer data to insurance agencies, background screeners, private detectives, law firms and even the federal government.

Some control is provided by the Gramm-Leach-Bliley Act of 1999, which governs the use of personal information maintained by financial institutions. And the Fair Credit Reporting Act of 1970, along with its 2003 amended version, the Fair and Accurate Credit Transactions Act, established rules for accessing and disseminating consumer reports.

But it has been a matter of debate over how those rules apply to vast information warehouses like ChoicePoint and LexisNexis, which offer a blend of both public and private information, only some of which is of interest to identity thieves.

The information services industry has lobbied hard in the past to stall legislation that would limit the kinds of information that can be peddled and to whom. But the succession of large-scale breaches, and the sheer number of consumers being affected by each new incident, could make it harder for the industry to resist some sort of legislative yoke.

"This is going to be hotly fought by people who are gathering and packaging this information," Mr. Barton said. "But I don't see why you have to have Social Security numbers available that are really extraneous to the product at hand."

Several new bills have been introduced in Congress to address concerns about consumer privacy, including three submitted in January by Senator Dianne Feinstein of California, a Democrat. Mr. Barton has said that he and colleagues from both parties have been discussing possible legislative approaches.

Senator Charles E. Schumer, Democrat of New York, who chastised another data compiler, WestLaw, in February for making sensitive information like Social Security numbers easily available, said he planned to introduce a bill next week.

"If we do nothing, identity theft is going to go through the roof," Mr. Schumer said yesterday. "It really means we should get on the stick and do something here. We're in the Wild West where companies can do anything they want."

LexisNexis and its parent company in London, the publishing and information services giant Reed Elsevier, said the recent breach involved databases acquired last July through the \$775 million purchase of Seisint, a compiler in Florida of consumer background and asset information.

Seisint has two main products: Accurint, a service for locating people and determining their assets, and Securint, a background screening service. LexisNexis has been in the process of folding those Seisint databases into its fleet of legal, news and consumer data archives.

Exactly how access was gained to the Seisint databases remains murky, but LexisNexis, which said the breach was discovered as part of "an ongoing extensive review of the verification, authorization and security procedures and policies," said that the breach appeared to have occurred well after the Seisint acquisition. The company also said it has been asked by law enforcement officials investigating the matter not to reveal too many details of the crime.

Kurt Sanford, the chief executive for corporate and federal markets at LexisNexis, which is based in Dayton, Ohio, emphasized that the company's own computer systems did not appear to have been

broken into by hackers.

Instead, Mr. Sanford said, it appears that thieves were able to secure the login names and passwords used by what he described as a handful of legitimate subscribers to the Seisint databases.

Mr. Sanford would not comment on whether the passwords were somehow stolen by hackers breaking into those customers' computers or were compromised by less technical means. But once logged in, the thieves were able to sift through a trove of consumer data without being detected until the legitimate subscribers were billed for their monthly activity.

In early February, Mr. Sanford said, those customers notified LexisNexis of the activities on their bills. The company took about two weeks to investigate the billing questions, Mr. Sanford said, and then notified law enforcement officials when it became clear that a break-in was involved. Reed Elsevier disclosed the breach in a public announcement yesterday morning in London.

The timing is of particular interest in the wake of the breach at ChoicePoint, which has been criticized for delaying notification of the 145,000 affected consumers for more than five months.

In that case, the company learned that it had been fooled by thieves posing as legitimate subscribers to its service in late September of last year. Law enforcement officials were notified, who said they asked the company to delay a public announcement. ChoicePoint did not publicly disclose the breach until mid-February.

LexisNexis said it planned to begin sending letters to the 30,000 consumers in the next few days, similar to the notification process that ChoicePoint recently completed.

More than one-third of the people whose data was compromised in the LexisNexis case appear to reside in California, according to a breakdown provided by the company. Massachusetts, New York, Florida and Texas were also heavily hit.

All 30,000 consumers will be offered free credit monitoring for one year, Mr. Sanford said. ChoicePoint made a similar gesture in notification letters that it mailed in the wake of the security breach there.

But privacy advocates argue that such gestures are not commensurate with the damage such security breaches can cause.

"Thieves will just put this stuff on the shelf until the heat is off," said Beth Givens, the director of the Privacy Rights Clearinghouse, a consumer advocacy group in San Diego.

"They know that there is increased scrutiny of these individuals at this time, and if they read the newspapers, they know that ChoicePoint and Lexis have purchased credit monitoring for one year," Ms. Givens said. "They need to tell these individuals that they need to be monitoring their credit for the rest of their lives."