

Statement by
Norman A. Willox Jr.
Chief Officer for Privacy, Industry and Regulatory Affairs
LexisNexis

March 30, 2005

**Before the California State Senate
Banking, Finance and Insurance Committee**

Good afternoon. My name is Norm Willox. I am Chief Officer for Privacy, Industry and Regulatory Affairs at LexisNexis. I appreciate the opportunity to be here today to discuss the important issues surrounding data security, privacy and the protection of consumer information.

LexisNexis is a leading provider of authoritative legal, public records, and business information. LexisNexis plays a vital role in supporting government, law enforcement and business customers who use our information services for important uses including: detecting and preventing identity theft and fraud, locating suspects, finding missing children and preventing and investigating criminal and terrorist activities.

LexisNexis products are used by financial institutions to help address the growing problem of identity theft and fraud. In 2004, 9.3 million consumers were victimized by identity fraud. Credit card companies report \$1 billion in losses each year from credit card fraud. With the use of a LexisNexis solution called Fraud Defender, a major bank card issuer experienced a 77 percent reduction in the dollar losses due to fraud associated with identity theft and credit card origination.

Our products are becoming increasingly necessary to combat identity fraud associated with internet transactions where high dollar merchandise such as computers and other electronic equipment are sold via credit card. Lower fraud costs ultimately mean lower costs and greater efficiencies for consumers.

LexisNexis products are also used to help prevent money laundering. LexisNexis has partnered with the American Bankers Association to develop a tool used by banks and other financial institutions to verify the identity of new customers to prevent money laundering and other illegal transactions used to fund criminal and terrorist activities.

Customers like the National Center for Missing and Exploited Children rely on LexisNexis to help them locate missing and abducted children. Since 1984, the Center has assisted law enforcement in recovering more than 85,000 children. Over the past 4 years, information provided by LexisNexis has been instrumental in a number of the Center's successful recovery efforts.

Finally, LexisNexis works closely with federal, state and local law enforcement agencies on a variety of criminal investigations. For example, the Beltway Sniper Task Force in Washington, D.C., used information provided by LexisNexis to help locate one of the suspects wanted in connection with that case. In another case, information provided by LexisNexis was recently used to locate and apprehend an individual who threatened a District Court Judge and his family in Louisiana. These are just a few examples of how our information products are used to help consumers by detecting and preventing fraud, strengthening law enforcement's ability to apprehend criminals, and enhancing our homeland security.

I would like to briefly describe the types of information contained in our databases. The information maintained by LexisNexis falls into three major categories: Public record information such as real estate records, professional licenses, and tax liens; publicly-available information such as telephone directories and newspaper reports; and non-public information such as social security numbers. The LexisNexis service does not include California driver's license information or any personal financial, credit, medical, or insurance information.

LexisNexis is committed to the responsible use of personally identifiable information. We have privacy policies and security measures in place to protect the consumer information in our databases. We limit access to full SSNs in non-public information to law enforcement clients, collections departments, financial institutions and special investigative units of insurance companies for the purposes of detecting, investigating and preventing fraud. Only those customers with a permissible purpose under federal and California law are granted access to this data.

LexisNexis has long recognized the importance of protecting the information in our databases and has multiple programs in place for verification, authorization and IT security. Maintaining security is not a static process -- it requires continuously evaluating and adjusting our security processes, procedures and policies.

As you know, LexisNexis recently reported a handful of data security incidents at Seisint, the information company we acquired last September. We sincerely regret these incidents and any adverse impact they may have on the individuals whose information may have been accessed.

We first discovered these incidents at Seisint in February when a LexisNexis integration team became aware of some billing irregularities and unusual usage patterns with several customer accounts. At that point we contacted the U.S. Secret Service. The Secret Service initially asked us to delay notification so they could conduct their investigation. About a week later we publicly announced these incidents and within a week sent out notices to consumers.

While the incidents are still being investigated, it appears that cybercriminals compromised IDs and passwords of legitimate Seisint customers and used them to access public records and certain personally identifying information, such as social security numbers. No California driver's license information or any personal financial, credit, or medical information was involved.

Following the discovery of these incidents, we took quick action to notify the approximately 30,200 individuals whose personal information may have been accessed and are providing them with a consolidated credit report and credit monitoring services. For those individuals who do become victims of fraud, we will provide counselors to help them clear their credit reports of any information relating to fraudulent activity. We will also provide them with identity theft expense insurance coverage up to \$20,000 to cover expenses associated with restoring their identity and repairing their credit reports.

Based on the incidents at Seisint, we have directed our teams to conduct a thorough review and examination of our records across all LexisNexis businesses to determine if there are any other incidents that potentially could have adversely impacted consumers.

As you know from recent news coverage and statistics from the California Office of Privacy Protection, data security breaches are not limited to information services companies. Universities, retailers and financial institutions comprise the majority of incidents that occur. Over the past week, two major California universities announced data security breaches. These two incidents combined resulted in the loss of personal information of over 150,000 alumni, faculty and students. A major retailer announced earlier this month the theft of credit card numbers and purchase information for over 100,000 consumers.

High-tech fraudsters are getting more sophisticated in the methods they use to access sensitive information in databases across all sectors. We have learned much from the security incidents at Seisint and are making changes in our business practices and policies, including enhancing ID and password administration procedures. Furthermore, we are educating our customers on ways they can increase their security.

LexisNexis is also committed to protecting the privacy of consumer information. In my role as Chief Privacy Officer, I work closely with our Privacy and Policy Review Board to protect the privacy of information contained in our databases. We also undertake regular assessments by independent third parties of both our privacy and security practices.

In addition, LexisNexis has a multi-layer process in place to screen potential customers to ensure that only legitimate customers have access to sensitive information. Our procedures include a detailed authentication process to determine the validity of business licenses, memberships in professional societies and other credentials.

Thank you again for the opportunity to discuss these very important issues. I would be happy to answer any questions the Committee may have.

###