Before the
U.S. House of Representatives
Committee on Financial Services

Hearing on
Assessing Data Security:
Preventing Breaches and Protecting Sensitive Information
May 4, 2005

Kurt P. Sanford
President and CEO
U.S. Corporate and Federal Government Markets
LexisNexis

Introduction

Good morning. My name is Kurt Sanford. I am the President and Chief Executive Officer for Corporate and Federal Markets 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. Today, over three million professionals—lawyers, law enforcement officials, government agencies employees, financial institution representatives, and others—use the LexisNexis services. Government agencies, businesses, researchers, and others rely on information provided by LexisNexis for a variety of important uses.

The following are examples of some of the important ways in which the services of LexisNexis are used by customers:

Preventing identity theft and fraud – Although the insidious effects of identity theft are fairly well known, until recently we did not fully appreciate that identity theft is part of the larger problem of identity fraud. Identity fraud, which encompasses identity theft, is the use of false identifiers, false or fraudulent documents, or a stolen identity in the commission of a crime. It is a component of most major crimes and is felt around the world today. As a result, both industry and government have asked LexisNexis to develop solutions to help address this evolving problem.

LexisNexis remains committed to providing leadership in this area. We recognize the enormity of the problem. 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.

LexisNexis 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.

Preventing 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. This tool allows banks to meet Patriot Act and safety and soundness regulatory requirements.

Locating suspects and helping make arrests – Many federal, state and local law enforcement agencies rely on LexisNexis to help them locate criminal suspects and to identify witnesses to a crime. 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.

Supporting homeland security efforts - LexisNexis worked with the Department of Homeland Security Transportation Safety Administration (TSA) in developing the Hazardous Materials Endorsement Screening Gateway System. This system allows TSA to perform background checks on commercial truck drivers who wish to obtain an endorsement to transport hazardous materials.

Locating and recovering missing children – 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.

Locating parents delinquent in child support payments – Both public and private agencies rely on LexisNexis to locate parents who are delinquent in child support payments and to locate and attach assets in satisfying court-ordered judgments. The Association for Children for the Enforcement of Support (ACES), a private child support recovery organization, has had tremendous success in locating nonpaying parents using LexisNexis.

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, protecting homeland security and assisting in locating missing and abducted children.

Types of Information Maintained by LexisNexis Risk Solutions

The information maintained by LexisNexis falls into the following three general classifications: public record information, publicly available information, and non-public information. I briefly describe each below.

Public record information. Public record information is information originally obtained from government records that are available to the public. Land records, court records, and professional licensing records are examples of public record information collected and maintained by the government for public purposes, including dissemination to the public.

Publicly available information. Publicly available information is information that is available to the general public from non-governmental sources. Telephone directories are an example of publicly available information.

Non-public information. Non-public information is information about an individual that is not obtained directly from public record information or publicly available information. This information comes from proprietary or non-public sources. Non-public data maintained by LexisNexis consists primarily of information obtained from either motor vehicle records or credit header data. Credit header data is the non-financial identifying information located at the top of a credit report, such as name, current and prior address, listed telephone number, social security number, and month and year of birth.

Privacy

LexisNexis is committed to the responsible use of personal identifying information. We have privacy policies in place to protect the consumer information in our databases. Our Chief Privacy Officer and Privacy and Policy Review Board work together to ensure that LexisNexis has strong privacy policies in place to help protect the information contained in our databases. We also undertake regular third-party privacy audits to ensure adherence to our privacy policies.

LexisNexis has an established Consumer Access Program that allows consumers to review information on them contained in the LexisNexis system. While the information provided to consumers under this program is comprehensive, it does not include publicly available information such as newspaper and magazine articles and telephone directories contained in the LexisNexis system.

LexisNexis also has a consumer opt-out program that allows individuals to request that information about themselves be suppressed from selected databases under certain circumstances. To opt-out of LexisNexis databases, an individual must provide an explanation of the reason or reasons for the request. Examples of reasons include:

- You are a state, local or federal law enforcement office or public official and your position exposes you to a threat of death or serious bodily harm;
- You are a victim of identity theft; or
- Your are at risk of physical harm.

Supporting documentation is required to process the opt-out request. While this opt-out policy applies to all databases maintained by our recently acquired Seisint business, it is limited

to the non-public information databases in the LexisNexis service. The policy does not currently apply to public records information databases maintained by LexisNexis. We are currently evaluating what steps we can take to better publicize our opt-out program and extend the program to all public records databases in the LexisNexis service.

Security

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. Preventive and detective technologies are deployed to mitigate risk throughout the network and system infrastructure and serve to thwart potentially malicious activities. LexisNexis also has a multi-layer process in place to screen potential customers to ensure that only legitimate customers have access to sensitive information contained in our systems. Our procedures include a detailed authentication process to determine the validity of business licenses, memberships in professional societies and other credentials. We also authenticate the documents provided to us to ensure they have not been tampered with or forged.

Only those customers with a permissible purpose under applicable laws are granted access to sensitive data such as driver's license information and social security numbers. In addition, customers are required to make express representations and warranties regarding access and use of sensitive information and we limit a customer's access to information in LexisNexis products according to the purposes for which they seek to use the information.

Maintaining security is not a static process -- it requires continuously evaluating and adjusting our security processes, procedures and policies. High-tech fraudsters are getting more sophisticated in the methods they use to access sensitive information in databases. We

continuously adapt our security procedures to address the new threats we face every day from those who seek to unlawfully access our databases. We undertake regular third-party security audits to test the security of systems and identify any potential weaknesses.

Even with the multi-layer safeguards in place at LexisNexis, we discovered earlier this year that unauthorized persons primarily using IDs and passwords of legitimate customers may have accessed personal identifying information at our recently acquired Seisint business. In February 2005, 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 approximately 30,000 individuals.

The investigation revealed that unauthorized persons, primarily using IDs and passwords of legitimate customers, may have accessed personal-identifying information, such as social security numbers (SSNs) and driver's license numbers (DLNs). In the majority of instances, IDs and passwords were stolen from Seisint customers that had legally permissible access to SSNs and DLNs for legitimate purposes, such as verifying identities and preventing and detecting fraud. No personal financial, credit, or medical information was involved since LexisNexis and Seisint do not collect such information. At no time was the LexisNexis or Seisint technology infrastructure hacked into or penetrated nor was any customer data residing within that infrastructure accessed or compromised.

Based on the incidents at Seisint, I directed our teams to conduct an extensive review of data search activity at our Seisint unit, and across all LexisNexis databases that contain

personal identifying information. In this review, we analyzed search activity for the past twenty-seven months to determine if there were any other incidents that potentially could have adversely impacted consumers. We completed that review on April 11, 2005. As a result of this in-depth review, we discovered additional incidents where there was some possibility that unauthorized persons may have accessed personal identifying information of approximately 280,000 additional individuals.

We deeply regret these incidents and any adverse impact they may have on the individuals whose information may have been accessed. We took quick action to notify the identified individuals. We are providing all individuals 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.

We have learned a great deal from the security incidents at Seisint and are making substantial changes in our business practices and policies across all LexisNexis businesses to help prevent any future incidents. These include:

- Changing customer password security processes to require that passwords for both system administrators and users be changed at least every 90 days;
- Suspending customer passwords of system administrators and users that have been inactive for 90 days;

- Suspending customer passwords after five unsuccessful login attempts and requiring them to contact Customer Support to ensure security and appropriate reactivation;
- Further limiting access to the most sensitive data in our databases by truncating SSNs displayed in non-public documents and narrowing access to full SSNs and DLNs to law enforcement clients and a restricted group of legally authorized organizations, such as banks and insurance companies; and
- Educating our customers on ways they can increase their security.

Laws Governing LexisNexis Compilation and Dissemination of Identifiable Information

There are a wide range of federal and state privacy laws to which LexisNexis is subject in the collection and distribution of personal identifying information. These include:

The Gramm-Leach-Bliley Act. Social security numbers are one of the two most sensitive types of information that we maintain in our systems and credit headers are the principal commercial source of social security numbers. Credit headers contain the non-financial identifying information located at the top of a credit report, such as name, current and prior address, listed telephone number, social security number, and month and year of birth. Credit header data is obtained from consumer reporting agencies.[1] The compilation of credit header data is subject to the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §§ 6801 *et seq*., and information subject to the GLBA cannot be distributed except for purposes specified by the Congress, such as the prevention of fraud.

[1] Consumer reporting agencies are governed by the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681 *et seq*. Some information services, such as Seisint's Securint service and LexisNexis PeopleWise, also are subject to the requirements of the FCRA.

Driver's Privacy Protection Act. The compilation and distribution of driver's license numbers and other information obtained from driver's licenses are subject to the Driver's Privacy Protection Act ("DPPA"), 18 U.S.C. §§ 2721 *et seq*., as well as state laws. Information subject to the DPPA cannot be distributed except for purposes specified by the Congress, such as fraud prevention, insurance claim investigation, and the execution of judgments.

Telecommunications Act of 1996. Telephone directories and similar publicly available repositories are a major source of name, address, and telephone number information. The dissemination of telephone directory and directory assistance information is subject to the requirements of the Telecommunications Act of 1996, as well as state law.

FOIA and other Open Records Laws: Records held by local, state, and federal governments are another major source of name, address, and other personally identifiable information. The Freedom of Information Act, state open record laws, and judicial rules govern the ability of LexisNexis to access and distribute personally identifiable information obtained from government agencies and entities. *See, e.g.,* 5 U.S.C. § 552.

Other laws:

Unfair and Deceptive Practice Laws: Section 5 of the Federal Trade Commission Act, and its state counterparts, prohibit companies from making deceptive claims about their privacy and security practices. These laws have served as the basis for enforcement actions by the Federal Trade Commission and state attorneys general for inadequate information security practices. The consent orders settling these enforcement actions typically have required

companies to implement information security programs that conform to the standards set forth in the GLBA Safeguards Rule, 16 C.F.R. Part 314.

Information Security Laws: A growing body of state law imposes obligations upon information service providers to safeguard the identifiable information they maintain. For example, California has enacted two statutes that require businesses to implement and maintain reasonable security practices and procedures and, in the event of a security breach, to notify individuals whose personal information has been compromised. *See* California Civil Code §§ 1798.81.5, 1798.82-84.

Legislative Measures LexisNexis Supports

We recognize that additional legislation may be necessary to further enhance data security and address the growing problem of identity theft and fraud. LexisNexis supports the following legislative approaches:

Data Security Breach Notification. We support requiring notification in the event of a security breach where there is substantial risk of harm to consumers. It is important that there is an appropriate threshold for when individuals actually would benefit from receiving notification, such as where the breach is likely to result in misuse of customer information. In addition, we believe that it is important that any such legislation contain federal preemption to insure that companies can quickly and effectively notify individuals and not struggle with complying with multiple, potentially conflicting and inconsistent state laws.

Adoption of Data Security Safeguards for Information Service Providers Modeled After the GLBA Safeguards Rule. LexisNexis supports the adoption of data security protections for information service providers modeled after the Safeguard Rule of the GLBA.

Increased penalties for identity theft and other cybercrimes and increased resources for law enforcement. LexisNexis strongly encourages legislation that imposes more stringent penalties for identity theft and other cybercrimes. Additionally, consumers and industry alike would benefit from enhanced training for law enforcement and an expansion of the resources available to investigate and prosecute the perpetrators of identity theft and cybercrime. Too many of our law enforcement agencies do not have the resources to neutralize these high-tech criminals.

Finally, LexisNexis strongly encourages that any legislation considered strike a balance between protecting privacy and providing legitimate businesses, organizations, and government agencies with access to critical information that enables them to fulfill their important missions.

I appreciate the opportunity to be here today to discuss the important issues surrounding data security, privacy and the protection of consumer information. I look forward to working with the members of this committee as you consider these important public policy issues.