

**CONFIDENTIAL**

December 6, 2012

The Honorable Michael A. Delaney  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

RE: Security Breach Notification

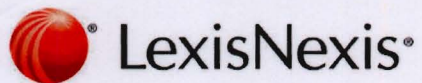
Dear Attorney General Delaney:

We are writing in accordance with your state's information security breach notification statute to inform you that we are notifying consumers of an incident in which a technical error led to sensitive personally identifiable information, including Social Security numbers and drivers' license numbers, about them being displayed in full in reports sent to other consumers. Typically, the Social Security numbers and drivers' license numbers would have been redacted. The issue began on October 30, 2012, was discovered on November 5, 2012 and was corrected by November 6, 2012.

We anticipate that notice will be sent to potentially affected consumers nationwide by United States mail on or about December 6, 2012. Among those to be notified are 3 residents of New Hampshire. A copy of the form notification letter is attached for your reference, and includes additional details about this matter.

We are offering potentially affected consumers one year of free credit monitoring, which is further detailed in the accompanying letter. We have also arranged for a specially trained support team to assist consumers who may have questions regarding this matter and/or the credit monitoring service.

Over the course of the last several years and since this occurrence, LexisNexis has taken a number of steps to strengthen its privacy and security safeguards to improve the overall protection of consumers' information. Some of the measures we have put in place include the implementation of a standards-based security control framework that drives protections for our network and access. LexisNexis has implemented numerous policies, procedures and standards that set forth clear parameters for data governance across the organization and for customers. LexisNexis also maintains a robust program of audit and compliance that serves as a system of checks and balances to assure that security controls are functioning efficiently and effectively, and that policies, procedures and standards are being followed. These protocols include controls for appropriate code development and testing and quality assurance. Despite these industry-leading security measures, an unfortunate error occurred and we have implemented additional precautions to strengthen our program.



If you have any questions regarding this matter, please contact me by telephone at 561-212-8034 or by electronic mail at [Linda.Clark@ReedElsevier.com](mailto:Linda.Clark@ReedElsevier.com).

Very truly yours,

A handwritten signature in blue ink that reads 'Linda K. Clark'.

Linda K. Clark  
Senior Counsel  
Data Security and Compliance

Enclosure

December 6, 2012

«FIRST» «MIDDLE» «LAST»  
«DELADDR»  
«CITY», «STATE» «ZIPCODE»

Dear «FIRST» «LAST»:

I am writing on behalf of LexisNexis Risk Solutions (a company that provides data services to insurance agencies, law enforcement agencies, and other industries) to inform you that sensitive personally identifiable information ("SPII") about you, including your full Social Security number and/or driver's license number, may have been included in a report sent to another individual.

On October 30, 2012, LexisNexis Risk Solutions implemented a technical change to a process used to generate reports. On November 5, 2012, LexisNexis Risk Solutions discovered that as an unintended consequence of this change, certain SPII which would have typically been partially masked was displayed in full in consumers' reports. In some cases, the reports contained SPII pertaining to other individuals involved in insurance claims shown on the report (for example, other members of the consumer's household or a person with whom the consumer experienced a vehicle collision).

The issue was promptly corrected on November 6, 2012, and additional remedial steps have been put in place to prevent recurrence.

We deeply regret this incident and any adverse impact it may have on you. We also want to provide as much information as possible to keep you fully informed.

Over the course of the last several years and since this occurrence, LexisNexis has taken a number of steps to strengthen its privacy and security safeguards to improve the overall protection of consumers' information. Some of the measures we have put in place include the implementation of a standards-based security control framework that drives protections for our network and access. LexisNexis has implemented numerous policies, procedures and standards that set forth clear parameters for data governance across the organization and for customers. LexisNexis also maintains a robust program of audit and compliance that serves as a system of checks and balances to assure that security controls are functioning efficiently and effectively, and that policies, procedures and standards are being followed. This includes controls for appropriate code development and testing and quality assurance. Despite these industry-leading security measures, an unfortunate error occurred and we have implemented additional precautions to strengthen our program.

#### **What We Recommend You Do**

LexisNexis is offering you a number of resources – free of charge – that will help you remain vigilant in monitoring free credit reports and detecting early signs of identity theft, as well as resolving any issues that may arise if your information was actually misused.

We have partnered with Experian, a nationwide credit bureau, to provide you with a full year of credit monitoring. This credit monitoring membership includes an initial Credit Report. It will enable you to identify possible fraudulent use of your information.

This credit monitoring product, ProtectMyID Elite, will identify and notify you of key changes to your credit file that could be a sign of identity theft. Your complimentary membership includes, for 1 year:

- One Bureau Credit Report on sign up.

- Monitoring of all three national credit reports (Experian, Equifax and TransUnion) every day.
- Internet scanning of online sources known for selling, trading, or sharing compromised data.
- Change of address monitoring checks.
- Email or SMS Text alerts when key changes are identified.
- \$1,000,000 identity theft insurance provided by Chartis, Inc.\*
- Access to Fraud Resolution Representatives.

\*Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of Chartis, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

You have until 02/28/2013 to activate this membership, which will then continue for twelve (12) months. We encourage you to activate your credit monitoring membership quickly. To redeem your membership, please visit: <http://www.protectmyid.com/enroll> or call 877-441-6943 and enter the code provided below.

Your Credit Monitoring Activation Code is: «CMCODE»

Additional information and support resources are available through the non-profit Identity Theft Resource Center at [www.idtheftcenter.org](http://www.idtheftcenter.org), by calling (858) 693-7935, or via e-mail at [itrc@idtheftcenter.org](mailto:itrc@idtheftcenter.org).

## Other Steps You Can Take

### ***Review Your Credit Reports Carefully***

When you receive your credit reports, please review them carefully. Look for inquiries you did not initiate, accounts you did not open and unexplained debts on the accounts you opened. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Contact information for the three national credit bureaus will be included with your report.

### ***Check For and Notify Credit Bureaus of Inaccuracies***

You also should check to see that information such as your most recent address(es), first and last names and middle initials are correct. Errors in this information may be warning signs of possible identity theft. You should notify the credit bureaus of all inaccuracies as soon as possible so the information can be investigated and, if found to be in error, corrected. Contact information for the three national credit bureaus is included below.

Bureau	Website	Address	Phone
Experian	<a href="http://www.experian.com">www.experian.com</a>	P.O. Box 2002, Allen, TX 75013	1-888-397-3742
Equifax	<a href="http://www.equifax.com">www.equifax.com</a>	P.O. Box 740241, Atlanta, GA 30374	1-888-766-0008
Transunion	<a href="http://www.transunion.com">www.transunion.com</a>	P.O. Box 6790, Fullerton, CA 92834	1-800-680-7289

Keep in mind, however, that inaccuracies in your credit report could also be due to simple mistakes. Nevertheless, if there are any inaccuracies in your reports or the information is incomplete in any way, you should notify the credit bureaus as soon as possible so the information can be investigated and, if found to be in error, corrected.

### ***Monitor Your Credit Report and Account Statements***

Remain vigilant. You should review your credit reports and financial account statements frequently, to make sure no fraudulent activity has occurred. With the ProtectMyID Elite credit monitoring service, all three of your national credit reports will be monitored on a daily basis and you will be notified if there are any important changes to your credit reports.

### ***Report Errors and Suspicious Activity to Your Creditors As Soon As Possible***

If you discover errors or suspicious activity on your credit report, you should immediately contact any credit card companies with which you have an account and inform them that you have received this letter. You should make sure the address they have on file is your current address and that any charges on the account were made by you. If you have not already done so, you should consider adding a personal identification number, or PIN, to your credit accounts. This will serve as an additional tool to protect your account and help the credit card company ensure they are only processing changes authorized by you.

### ***Place a Security Alert on Your Credit Reports***

We recommend before requesting a security alert that you review all items on your credit reports for inaccuracies. Although a security alert service will warn potential creditors to take additional precautions when reviewing your credit

records or applications for additional credit, be aware that it could take longer for you to obtain new credit. If you want to renew the security alerts, the three national credit bureaus will require you to contact each organization separately.

**Contact the FTC, your state Attorney General, or local law enforcement.**

You can obtain additional information about fraud alerts and security file freezes from the three national credit bureaus, the Federal Trade Commission ("FTC"), or your state Attorney General's office.

In addition, if you believe that you have been a victim of identity theft you can file a report with the Federal Trade Commission (FTC), 600 Pennsylvania Ave NW, Washington DC, 20580, <http://www.consumer.gov/idtheft/> or at (877) ID-THEFT (438-4338). Your report will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. Also, at <http://www.consumer.gov/idtheft/>, you may download a copy of Take Charge: Fighting Back Against Identity Theft, a comprehensive guide from the FTC to help you guard against and deal with identity theft.

By way of background, the FTC is the federal agency charged with protecting consumers from deceptive, unfair, and anticompetitive trade practices that harm consumer welfare. Consistent with this mission, the FTC, among its many other responsibilities, is responsible for the enforcement efforts required to safeguard consumers' privacy and personal information.

You also may be able to obtain additional information about identity theft from, and report suspected identity theft to, your state Attorney General's office and/or local law enforcement.

Maryland Residents: For additional information about identity theft, in addition to the FTC, credit bureaus, and other sources above, you also may contact: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202. [www.oag.state.md.us](http://www.oag.state.md.us). (888) 743-0023.

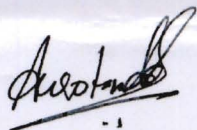
North Carolina Residents: For additional information about identity theft, in addition to the FTC, credit bureaus, and other sources above, you also may contact: North Carolina Department of Justice, Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001. <http://www.ncdoj.gov/>. (919) 716-6750.

**Contact us for additional information.**

We hope this information is helpful to you and again we sincerely regret any adverse impact this incident may have on you.

We have arranged for a specially trained support team to assist you with questions regarding this matter. This team is available from 6 a.m. – 6 p.m. PST, Monday through Friday, and 8 a.m. – 5 p.m. PST, Saturday and Sunday at 877-441-6943. They are available to answer your questions regarding this notice, help you order your Credit Report and set up your credit monitoring membership.

Sincerely,



Aurobindo Sundaram  
Vice President - Security, Investigations, and Incident Response  
Reed Elsevier Inc.  
1000 Alderman Dr, Suite 280  
Alpharetta, GA 30005