

MICHAEL C. LAMB, ESQ.
VICE PRESIDENT AND LEAD COUNSEL - REGULATORY, PRIVACY AND POLICY
LEXISNEXIS® RISK SOLUTIONS

May 9, 2011

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

RE: Security Breach Notification

Dear Attorney General Delaney:

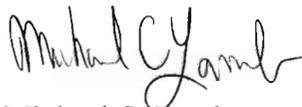
We are writing in accordance with your state's information security breach notification statute to inform you that we are notifying consumers of an incident in which sensitive personal information about them accessed by Onyx Collections & Locators Services Inc., located in Atlanta, Georgia ("Onyx"), may have been viewed by an individual who should not have had access to such information. We anticipate that notice will be sent to potentially affected consumers nationwide by United States mail on or about May 9, 2011. Among those to be notified are 74 residents of New Hampshire. A copy of the form notification is attached for your reference.

From September 10, 2009 through March 2, 2011, Onyx had access to personally identifiable information for individuals who are residents in New Hampshire. This information may have included names, addresses, dates of birth, driver's license numbers and/or social security numbers of potentially affected consumers. Recently, LexisNexis conducted an audit of Onyx the result of which has caused us concern that there is a risk of misuse of personal information accessible in the data services we provided to Onyx.

Prior to contacting you, LexisNexis was working with federal law enforcement to further investigate this matter. LexisNexis was advised to delay consumer notices in order to facilitate law enforcement's investigation. However, we have now received authorization to send notice to consumers and we are promptly doing so. In addition to notification, we are offering potentially affected consumers one year of free credit monitoring, which is further detailed in the accompanying letter that we are sending to potentially affected state residents by United States mail, and which is attached hereto. 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. This team will be available to answer questions regarding the notice, help consumers order their Three-Bureau Credit Report, and set up their credit monitoring membership.

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, access, and monitoring of product use to detect and respond to potentially fraudulent activity. Additionally, prospective customers must undergo a process of verification or "credentialing" to affirm that the prospective user is a legitimate business with a permissible purpose to access the information. 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 audit and compliance program that serves as a system of checks and balances to ensure that security controls are functioning efficiently and effectively, and that policies, procedures and standards are being followed.

Very Truly Yours,



Michael C. Lamb

[Date]

[Consumer Name]

[Address]

[City], [State] [ZIP code]

Dear [Consumer Name]:

I am writing to inform you that sensitive personally identifiable information about you may have been viewed by an individual who should not have had access to such information. LexisNexis provides data services to law enforcement agencies, collections agencies and other industries. Recently, LexisNexis audited a collections agency customer, Onyx Collections & Locators Services Inc., located in Atlanta, Georgia (“Onyx”). The audit response that we received from Onyx, as well as other information that we have gathered, causes us concern that there is a risk of misuse of your personal information that was accessible in the data services we provided to Onyx. Therefore, and in an abundance of caution, LexisNexis is notifying all consumers whose information may have been viewed by Onyx through Onyx’s access to our services so that you may take appropriate steps to protect your identity and also to offer you a series of free support services.

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.

What Information May Have Been Viewed, When and By Whom

From September 10, 2009 through March 2, 2011, Onyx had access to information that may have included your name, address, date of birth, driver’s license number and/or social security number.

LexisNexis is working with federal law enforcement to further investigate this matter. LexisNexis was advised to delay consumer notices in order to facilitate law enforcement’s investigation. However, we have now received authorization to send this letter. If you have experienced or later detect any misuse of your personal information, please contact us immediately at (866) 252-0121 so that we may provide this information to law enforcement.

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, access, and monitoring of product use to detect and respond to potentially fraudulent activity. Additionally, prospective customers must undergo a process of verification or “credentialing” to affirm that the prospective user is a legitimate business with a permissible



purpose to access the information. 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. Despite these industry-leading security measures, there is a risk that data misuse by Onyx or an Onyx employee occurred.

What We Recommend You Do

LexisNexis is offering you a number of resources – free of charge – that will help you detect early signs of identity theft, as well as resolve any issues that may arise if your information was actually misused.

We have partnered with ConsumerInfo.com, Inc., an Experian® company, to provide you with a full year of credit monitoring. This credit monitoring membership includes an initial Three-Bureau Credit Report. It will enable you to identify possible fraudulent use of your information.

This credit monitoring product, Triple AdvantageSM, will identify and notify you of key changes that may be a sign of identity theft. Your complimentary membership includes:

- One Three-Bureau Credit Report when you sign up.
- Unlimited access to your Experian Credit Report and Credit Score.
- Monitoring of all three of your national credit reports (Experian, Equifax and TransUnion) every day.
- Email or SMS Text alerts when key changes are identified.
- \$25,000 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.

We have also arranged for a specially trained support team to assist you with questions regarding this matter and the Triple Advantage product. 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 (866) 252-0121. They are available to answer your questions regarding this notice, help you order your Three-Bureau Credit Report and set up your credit monitoring membership.

You have until July 15, 2011 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://partner.consumerinfo.com/premium> and enter the

code provided below. You will be instructed on how to initiate your online membership. To the extent you do not have access to the Internet, please contact the specially trained support team, referenced in the previous paragraph, to activate a similar product via the telephone as well as to answer any questions or address any concerns you have. Support team members are available by calling toll free to (866) 252-0121 during the time period referenced in the paragraph above.

Your Credit Monitoring Activation Code is: [*Unique code for each consumer to be input upon production*]]. Please activate it at: <http://partner.consumerinfo.com/premium>

Additional information and support resources are available through the non-profit Identity Theft Resource Center at www.idtheftcenter.org, by calling (858) 693-7935, or via e-mail at 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 will be included with your report.

Keep in mind, however, that inaccuracies in this information may also be due to simple mistakes. Nevertheless, if there are any inaccuracies in your reports, 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

You should check your credit reports frequently for the next year, to make sure no new fraudulent activity has occurred. With the Triple Advantage 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 consider immediately contacting any credit card companies with which you have an account and tell 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.

File a Complaint with the FTC

You may file a complaint with the Federal Trade Commission (FTC) at <http://www.consumer.gov/idtheft/> or at (877) ID-THEFT (438-4338). Your complaint 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.

We hope this information is helpful to you and 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 (866) 252-0121. They are available to answer your questions regarding this notice, help you order your Three-Bureau Credit Report and set up your credit monitoring membership.

Sincerely,

Aurobindo Sundaram
Vice President, Security, Investigations, and Incident Response