

May 7, 2009

This letter from LexisNexis was sent to potential victims whose information may have been compromised.

I am writing to inform you that sensitive personally identifiable information about you may have been viewed by a few individuals who should not have had access to such information. These individuals were operating businesses that at one time were both ChoicePoint and LexisNexis (hereafter "LexisNexis") customers, but are no longer. Please be aware that the United States Postal Inspection Service, a federal law enforcement agency investigating this matter, has already notified you directly if it has reason to believe you have been an actual victim of a crime.

We want to provide as much information as possible to keep you fully informed.

What Information May Have Been Viewed, When and By Whom

LexisNexis was contacted by the United States Postal Inspection Service ("USPIS") concerning an ongoing investigation into alleged credit card fraud perpetrated by the above-mentioned former customers of LexisNexis. By utilizing fraudulently-opened mail boxes at commercial mail receiving businesses and personal information of United States residents obtained via LexisNexis, these individuals were able to apply for and obtain fraudulent credit cards. The unauthorized access to personal information by the former LexisNexis customers may have occurred sometime between June 14, 2004, and October 10, 2007, and the information accessed may have included your name, date of birth, and/or social security number.

In order to preserve the integrity of the criminal investigation, the USPIS instructed LexisNexis to delay notifying you until the completion of the USPIS investigation. This letter is the first opportunity to share information with those whose information may have been viewed, but for whom the USPIS has advised us that there is no evidence of identity fraud. If you are among those who have been identified as a victim of credit card fraud by USPIS, you have already been notified by the USPIS.

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. We also limit access to sensitive personally identifiable information except where there is a critical business need coupled with a permissible purpose for such access. Additionally, prospective customers must undergo a multi-stepped, rigorous process of verification or "credentialing," including site visits in many instances, to affirm that the prospective user is a legitimate business with permissible purpose. 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.

How We Can Help

LexisNexis would like to offer you a number of resources - free of charge to you -- 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 any 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 every day.
- Email or SMS Text alerts when key changes are identified.
- \$25,000 identity theft insurance provided by Virginia Surety Company, Inc.*
- Access to Fraud Resolution Representatives.

*Coverage cannot be offered to residents of New York.

We have also arranged for a specially trained support team to assist you with the use of and questions regarding the Triple Advantage product from 6 a.m. to 6 p.m. PDT, Monday through Friday, and 8 a.m. to 5 p.m. PDT, Saturday and Sunday at (888) 829-6551. They are available to help you order your Three-Bureau Credit Report and set up your credit monitoring membership.

You have ninety (90) days from the date of this letter 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/uspis> and enter the code provided below, disregarding any pricing information. 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. Such team members are available at the following toll-free number (888)-829-6551 during the time period referenced in the paragraph above.

Your Credit Monitoring Activation Code is: [INSERT UNIQUE CODE HERE]. Please activate your complimentary credit monitoring service here: <http://partner.consumerinfo.com/uspis>.

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 Inaccuracies and Notify Credit Bureaus of Them

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 can 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 also may be due to simple mistakes. Nevertheless, if there are any inaccuracies in your reports, whether due to fraud or error, 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 continue to 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 have discovered errors or suspicious activity on your credit report, you should consider immediately contacting any credit card companies with whom 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.

Contact The United States Postal Inspection Service ("USPIS")

If an unauthorized account has been opened in your name, and you have not previously been contacted by the USPIS, a special hotline, (800) 372-8347, has been established for you to report the account to address any law enforcement related questions or concerns you might have. Once your call is answered you will be directed to the main menu, and at that time you will need to press 8 to reach the USPIS message related to this specific investigation. The USPIS hotline will be active Monday through Friday, from 8:00 a.m. to 5:00 p.m., Central Standard Time. Upon receipt of your call, you will be asked to leave a message that includes your full name, daytime phone number, mailing address, and the financial institution where you believe the suspicious account is held. The USPIS will then contact you for further follow-up.

File a Complaint with the FTC

You may file a complaint with the Federal Trade Commission (FTC) at 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 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 which 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 inconvenience this may cause you.

Sincerely,

By Ariel Bashi

© MMIX, CBS Interactive Inc. All Rights Reserved.