



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

January 25, 2022

Via Email

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566
Email: ldtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP ("Lewis Brisbois") represents Nansemond Insurance Agency ("Nansemond") in connection with a recent data security incident described in greater detail below.

1. Nature of the security incident.

On September 14, 2021, Nansemond experienced an incident resulting in unauthorized access to certain of its systems. In response, Nansemond took immediate steps to secure its systems and promptly launched an investigation. In so doing, Nansemond engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization. As a result, Nansemond learned that personal information belonging to certain customers / employees associated therewith was impacted in connection with the incident. Nansemond then took steps to identify such individuals and to locate current mailing addresses in order to effectuate notification.

The information that may have been accessible by the malicious actor(s) responsible for this incident includes individuals' names, drivers' license numbers, and Social Security numbers.

2. Number of Maryland residents affected.

Nansemond notified 1 Maryland resident of this incident via first class U.S. mail on January 25, 2022. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as Nansemond discovered this incident, Nansemond took steps to secure its systems and launched an investigation to determine what happened and whether personal information had been

January 25, 2022

Page 2

accessed or acquired without authorization. Nansemond has also implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future.

Nansemond has established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at 1-800-939-4170 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays). In addition, while Nansemond is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Nansemond is also providing complimentary identity protection services to notified individuals.

4. Contact information.

Nansemond remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Lewis Brisbois.

Best regards,

A handwritten signature in blue ink, appearing to read 'Alyssa R. Watzman'.

Alyssa R. Watzman
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter

Nansemond Insurance Company

10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:

1-800-939-4170

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code:

<<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

January 25, 2022

Subject: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

We at Nansemond are committed to protecting the confidentiality and security of the information we receive and maintain. We are writing to inform you of a recent data security incident we experienced that may have involved some of your information. Nansemond may have retained your information on behalf of your employer, which has commercial truck insurance through Nansemond Insurance Agency. While we are unaware of any misuse of your information, we are notifying you of the incident, offering you complimentary credit monitoring and identity protection services, and informing you about steps you can take to help protect your personal information.

What Happened: On September 14, 2021, Nansemond learned of a security incident that resulted in unauthorized access to our digital environment. Upon discovering this unauthorized activity, we immediately secured our digital environment and began to investigate. We also engaged a leading computer forensic firm and cybersecurity experts to address the incident, restore operations, and conduct an investigation. The investigation revealed that an unauthorized party acquired certain files and data stored on Nansemond's computer servers.

What Information Was Involved: Nansemond completed a comprehensive review of the data that could have potentially been acquired by the unauthorized party and determined that information included your name and driver's license number.

What We Are Doing: To help prevent something like this from happening again, we are implementing additional technical security measures and increasing employee cybersecurity training. While we have no indication that your information has been misused, we are nonetheless providing you with information about steps that you can take to help protect your personal information. As a further precaution, we are also offering you **one year** of complimentary credit and identity monitoring services through IDX. This product helps detect possible misuse of your information and provides you with identity protection support.

What You Can Do: You can enroll in IDX's complimentary credit and identity monitoring services by going to <https://app.idx.us/account-creation/protect> or calling 1-800-939-4170. When prompted, please provide the following unique enrollment code <<XXXXXXXXXX>> to enroll in the services. The deadline to enroll is April 25, 2022. For more information on how you can protect your personal information, please review the resources provided on the following pages.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-800-939-4170 between 9 am to 9 pm Eastern Time.

The security of your information is a top priority for Nansemond. We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Joby Webb

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 2000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

How do I place a freeze on my credit reports? You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact each of the credit reporting agencies identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

How do I lift a freeze from my credit reports? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional information for residents of the following states:

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202, 1-888-743-0023, oag.state.md.us.

North Carolina: North Carolina Attorney General can be reached at: 9001 Mail Service Center, Raleigh, NC 27699, ncdoj.gov.