PIERSON FERDINAND

ELIZABETH DELNEGRO
PARTNER [PT]

Mail
1625 E Maryland Ave
Phoenix, AZ 85016

Office
2 North Central Ave, Suite 1800
Phoenix, AZ 85004

Direct: 480.550.9433
Email: elizabeth.delnegro@pierferd.com

September 24, 2025

VIA EMAIL (DOJ-CPB@doj.nh.gov)
Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General Formella:

Pierson Ferdinand LLP represents Nusbaum Insurance Agency ("Nusbaum") located at 403 Boush St., Ste 300, Norfolk, VA 23510, in connection with a data security incident described in more detail below. The protection and proper use of information in its possession is a top priority for Nusbaum, and Nusbaum has taken steps to prevent a similar incident from occurring again in the future.

1. Description of the incident

In August 2024, Nusbaum experienced a data security incident in which an unauthorized third party gained access to Nusbaum's email environment. Nusbaum initiated its incident response plan, engaged its third-party IT provider, and commenced an investigation. The third-party IT team secured its environment, hardened and enhanced its network security, and completed an investigation to ensure that Nusbaum's email environment was secure.

Following Nusbaum's third-party IT investigation, Nusbaum engaged additional third-party experts. These specialized third parties confirmed that its environment was secured and made additional enhancements to Nusbaum's network security. The specialized third parties also completed a digital forensic investigation in which they were able to discover and determine the full extent of unauthorized activity within Nusbaum's entire network.

The forensic investigation determined that certain customer emails containing personal or health information could have been available for unauthorized access. Impacted data elements vary for each individual – the following personal information for your state's residents could have been impacted by this incident: name; Social Security number; Driver's License number; date of birth; and health or medical information.

2. Steps taken

Nusbaum is committed to ensuring the security and proper use of all information in its control. Nusbaum worked with experts to investigate how the incident occurred and take appropriate remedial and hardening steps to enhance network security and data privacy.

Nusbaum commenced an extensive third-party data mining project to identify potentially impacted individuals, identified data elements, and mailing addresses. Notification letters were mailed to 3 residents of your state on September 11, 2025. A sample copy of the notification letter is attached as Exhibit A. This notification included complimentary credit monitoring and identity protection services for twelve (12) months through CyEx, a company specializing in fraud assistance and remediation services. At this time, Nusbaum is not aware of any personal information having been misused as a result of this incident.

3. Contact information

Nusbaum remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at Elizabeth Delnegro at elizabeth.delnegro@pierferd.com or +1(360) 402-0834.

Sincerely,

PIERSON FERDINAND

Elizabeth A. Delnegro

EAD
Enclosures (1)

EXHIBIT A

NUSBAUM INSURANCE

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

<<Variable Data 1>>

Dear <<Full Name>>,

Nusbaum Insurance Agency ("Nusbaum" or "we") recently experienced a data security incident that may have affected your personal information. We want to make you aware of the incident and the measures we have taken in response, as well as provide details on steps you can take – should you deem it appropriate – to help protect your information. The protection, privacy, and proper use of your information is a top priority for us, and we are committed to preventing this type of incident from occurring again.

What Happened

On or about August, 2024, Nusbaum experienced a data security incident in which an unauthorized third party gained access to Nusbaum's email environment. We immediately initiated our incident response plan, engaged our third-party IT provider, and commenced an investigation. The third-party IT team secured our environment, hardened and enhanced our network security, and completed an investigation to ensure that our email environment was secure. Following our own third-party IT investigation, we engaged additional third-party experts. These specialized third parties confirmed that our environment was secured, made additional enhancements to our network security, and completed a digital forensic investigation to determine the full extent of unauthorized activity within Nusbaum's entire network. Unfortunately, these types of incidents have become increasingly common and even organizations with the most sophisticated IT infrastructure available are affected. We have worked diligently to determine what happened and what information could have been compromised.

What Information Was Involved

The third-party digital forensic investigation determined that an unauthorized party could have had access to your personal information. The elements of your personal information that may have been compromised include: <<Breached Elements>>. Please note that we have no evidence at this time that any personal information has been misused as a result of the incident.

What We Are Doing

We take data privacy seriously and are committed to continuing to strengthen our systems' security to prevent a similar event from occurring in the future. We are also focused on enhancing our cyber preparedness through additional awareness training and updating our procedures. Nusbaum also notified law enforcement regarding this incident.

Additionally, out of an abundance of caution, we have arranged for you to activate complimentary credit monitoring and identity restoration services at no charge to you. These services provide alerts for <<CM Duration>> months through CyEx. These services will be provided by CyEx Identity Defense Complete, a company specializing in fraud assistance and remediation services.

What You Can Do

To enroll in the complimentary services we are offering you, please follow the instructions provided. For you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter, no later than **<<Enrollment Deadline>>**. You can enroll by using enrollment code **<<Activation Code>>** and visiting: ***app.identitydefense.com/enrollment/activate/Nusbaum***

Please note that to activate monitoring services, you will need an internet connection and e-mail account. Additionally, you may be required to provide the appropriate name, date of birth, and Social Security number to confirm identity and authority. Due to privacy laws, we cannot register you directly. Please note that certain services might not be available for individuals who do not have a credit file with the credit bureaus or an address in the United States (or its territories) and a valid Social Security number. Activating this service will not affect your credit score. If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

At this time, we are not aware of anyone experiencing fraud as a result of this incident. As data incidents are increasingly common, we encourage you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of personal information. We encourage you to review the Additional Important Information located on the following pages, which includes further steps to safeguard your personal information, such as implementing a fraud alert or security freeze. We also recommend validating the sender of any emails and being wary of phishing attempts.

For More Information

Please know that Nusbaum Insurance Agency values the protection and privacy of your personal information, and we understand the concern and inconvenience this incident may cause. If you have any questions, call 877-332-1723 between 9:00 a.m. - 9:00 p.m. Eastern time, Monday through Friday, excluding holidays.

Sincerely,

Michael Nusbaum

Vice President

Nusbaum Insurance Agency

Identity Defense

<<Full Name>>
Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>
Service Term: <<CM Duration>> months *

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

To enroll in Identity Defense, visit app.identitydefense.com/enrollment/activate/Nusbaum

1. Enter your unique Activation Code <<Activation Code>>
   Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
   Enter your email address, create your password, and click 'Create Account'.
3. Register
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>**.** After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by** <<Enrollment Deadline>>**, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.
**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, 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.

Additional Important Information

Monitoring: You should always remain vigilant and monitor your accounts for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for suspicious or unusual activity. You can report suspicious activity to financial institutions or law enforcement.

Fraud Alert: You can place fraud alerts with the three major credit bureaus by phone and online as set forth below with Equifax, TransUnion, or Experian. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can get an extended fraud alert for seven years.

Credit Report: Consumers are also entitled to one free credit report annually from each of the three credit reporting bureaus. To order your free credit report: visit www.annualcreditreport.com; call, toll-free, 1-877-322-8228; or mail a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information may need to be included when requesting a security freeze: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current and addresses for the past five years; (5) proof of address; (6) Social Security Card, pay stub, or W2; or (7) government-issued identification card. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	Equifax	TransUnion
1-888-397-3742	1-800-349-9960	1-888-909-8872
www.experian.com/help/	www.equifax.com/personal/credit-report-services/	www.transunion.com/credit-help
Fraud Alert P.O. Box 9554 Allen, TX 75013	Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Fraud Alert P.O. Box 2000 Chester, PA 19016
Credit Freeze P.O. Box 9554, Allen, TX 75013	Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788	Credit Freeze P.O. Box 160, Woodlyn, PA 19094

Implementing an Identity Protection PIN (IP PIN) with the IRS: To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register and validate your identity. Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. Some items to consider when obtaining an IP PIN with the IRS: (1) an IP PIN is valid for one calendar year; (2) a new IP PIN is generated each year for your account; (3) logging back into the Get an IP PIN tool, will display your current IP PIN; and (4) an IP PIN must be used when filing any federal tax returns during the year including prior year returns.

Fair Credit Reporting Act: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Federal Trade Commission: More information can be obtained by contacting the Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

***For Massachusetts residents*:** You can obtain a police report if you are a victim of identity theft.

***For Iowa residents*:** You can report any suspected identity theft to law enforcement or to the Attorney General.

***For Rhode Island residents*:** You can obtain a police report if you are a victim of identity theft and contact the Rhode Island Office of the Attorney General at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; www.riag.ri.gov.

***For Oregon residents*:** You can report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

***For Vermont residents*:** If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Residents of the below states can obtain additional information regarding identify theft and more at:

- ***District of Columbia Attorney General***: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and https://oag.dc.gov.
- ***Maryland Office of the Attorney General***: Consumer Protection Division, 200 St. Paul Place, 16th Fl, Baltimore, MD 21202; 1-888-743-0023; https://www.marylandattorneygeneral.gov/.
- ***New York Attorney General***: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.
- ***North Carolina Attorney General***: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and https://www.ncdoj.gov.