



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Angelina W. Freind
Office: (267) 930-4782
Fax: (267) 930-4771
Email: afreind@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 4, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Johns Eastern Company, Inc. (“JEC”), located at PO Box 110259, Lakewood Ranch, Florida 34211, and are writing to notify your office of an incident that may affect the security of some personal information relating to one hundred seven (107) Maryland residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, JEC does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On December 1, 2021, JEC discovered unusual activity on its computer network. Upon discovery of the event, JEC immediately launched an internal investigation to confirm the full nature and scope of what occurred. JEC worked tirelessly with third-party forensic specialists to investigate and respond to this incident, as well as to restore operations. Additionally, JEC reported the incident to the Federal Bureau of Investigation (FBI) and are cooperating, as required.

The investigation confirmed that JEC was the victim of a sophisticated cyberattack. As part of the response, JEC worked with the forensic teams to assess whether any personal information may have been impacted as a result of this event. This included analyzing the affected systems and reviewing data stored within the JEC environment. The investigation confirmed on or about December 20, 2021 that personal data may have been accessed or viewed by an unauthorized third party as a result of this event.

The information that could have been subject to unauthorized access includes name, Social Security number, and date of birth.

Notice to Maryland Residents

On or about January 4, 2022, JEC began providing written notice of this incident to affected individuals, which includes one hundred seven (107) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, JEC moved quickly to investigate and respond to the incident, assess the security of JEC systems, and notify potentially affected individuals. JEC is also working to implement additional safeguards and training to its employees. JEC is providing access to credit monitoring services for one (1) year, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, JEC is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. JEC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4782.

Very truly yours,

Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF/cob
Enclosure

EXHIBIT A



JOHNS EASTERN

Claim Adjusters & Third Party Administrators

PO Box 110259, Lakewood Ranch, FL 34211-0004

January 4, 2022

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

NOTICE OF SECURITY INCIDENT

Dear <<Name 1>> <<Name 2>>:

Johns Eastern Company, Inc ("JEC") is writing as a follow up to our previous communications regarding an incident that could affect the security of some of your personal information. You are receiving this letter because you or one of your family members works for JEC and were previously provided with information regarding a recent event impacting JEC's systems. While we are unaware of any actual or attempted misuse of your information, we take this incident very seriously and we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so. This letter is intended to supplement the communications previously provided to you or your family member and does not relate to a new incident.

What Happened? On December 1, 2021 JEC discovered unusual activity on its computer network. Upon discovery of the event, JEC immediately launched an investigation to confirm the full nature and scope of what occurred. We worked tirelessly with third-party forensic specialists to investigate and respond to this incident, as well as to restore our operations. Additionally, we reported the incident to the FBI and are cooperating, as required.

The investigation confirmed that JEC was the victim of a sophisticated cyberattack. As part of our response, we worked with the forensic teams to assess whether any personal information may have been impacted as a result of this event. This included analyzing the affected systems and reviewing data stored within the JEC environment. Our investigation confirmed on or about December 20, 2021 that your personal data may have been accessed or viewed by an unauthorized third party as a result of this event.

What Information Was Involved? Again, we have no evidence of any identity theft or fraud connected to this event, but because your data may have been accessed, we are notifying you out of an abundance of caution. Our investigation confirmed that the data present in the impacted systems may include your name, date of birth and Social Security number. If you participated in JEC's health plan, your insurance group number may also have been impacted.

What We Are Doing. Addressing this incident has been JEC's utmost priority. We have security measures in place to protect the data on our systems and we continue to assess and update security measures and employee

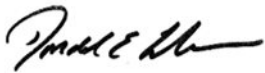
training to safeguard the information in our care. As part of our ongoing commitment to the security of information, we are also reviewing our policies and procedures to examine existing security measures.

We previously offered you 12 months of complimentary credit monitoring services through TransUnion. While we still have no evidence of any misuse of your information related to this event, we wanted to provide you with these services as a precaution. If you did not already enroll in these services, you can do so now. To enroll, please refer to the instructions below. These services include fraud consultation and identity theft restoration services. We encourage you to activate these services as we are unable to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. We also encourage you to review the “*Steps You Can Take to Protect Personal Information*” section of this letter, which describes steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. Further, we encourage you to activate the credit monitoring services through TransUnion.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 800-767-9480, Ext. 1970. You may also write to JEC at PO Box 110259, Lakewood Ranch, FL 34211-0004 or JECreditmonitoring@johnseastern.com.

Sincerely,



Donald E. Lederer
President and Chief Executive Officer
Johns Eastern Company, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring



Activation Code: **ACTIVATION CODE**

3-Bureau Credit Monitoring Product Offering: (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online 3-bureau credit monitoring service (*myTrueIdentity*) for 12 months provided by TransUnionInteractive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code: **ACTIVATION CODE** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, 3-bureau credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone **PASSCODE**, and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain 12 months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily 3- bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian® and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *myTrueIdentity* online 3-Bureau Credit Monitoring service anytime between now and **March 31, 2022**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit files at TransUnion®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *myTrueIdentity* online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If

you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this incident.