

May 7, 2021

Norton Rose Fulbright US LLP
1301 McKinney, Suite 5100
Houston, Texas 77010-3095
United States

Via E-mail (DOJ-CPB@doj.nh.gov)

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Direct line +1 713 651 5684
will.daugherty@nortonrosefulbright.com

Tel +1 713 651 5151
Fax +1 713 651 5246
nortonrosefulbright.com

Dear Sir or Madam:

I am writing on behalf of my client, JHT Holdings, Inc. ("JHT"), to provide notice of a security incident that occurred at JHT.¹ JHT is the parent company to a number of subsidiaries including, Auto Truck Transport LLC, Active Truck Transport LLC, Equipment Transfer LLC, ATC Transportation LLC, and Unimark Truck Transport LLC.

On March 22, 2021, JHT and its subsidiaries discovered that it was the target of a ransomware attack in which an unauthorized actor used malware to encrypt certain servers. JHT took steps to secure its systems, launched an investigation, and a cybersecurity firm was engaged to assist. JHT also notified the Federal Bureau of Investigation.

JHT's investigation determined that the unauthorized actor gained access to certain systems within its environment at various times from approximately March 4, 2021 to March 22, 2021. During this time period, the unauthorized actor appears to have obtained data from certain JHT systems. On April 15, 2021, JHT learned that the data obtained by the unauthorized actor may have contained personal information relating to current and former employees and applicants of JHT's subsidiaries, including names, Social Security numbers, and DOT required drug test results of 11 New Hampshire residents.

Today, JHT's subsidiaries are sending notification letters via First Class Mail to the 11 New Hampshire residents whose information may have been involved in the incident. This notice is being provided in accordance with New Hampshire Revised Statute §359-C:20. Enclosed is a sample copy of the letter. JHT is offering one year of complimentary credit monitoring and identity protection services from TransUnion as well as a toll free hotline for the individuals to call with any questions they may have.

To help prevent a similar incident from occurring in the future, JHT implemented additional security measures designed to enhance the security of its network, systems, and data, including isolating systems believed to be compromised or encrypted; eradicating malicious files; forcing password resets; enhancing network restrictions; deploying an advanced endpoint monitoring tool. JHT also continues to evaluate additional steps that may be taken to further increase its defenses going forward.

¹ This notice is not, and does not constitute, a waiver of JHT's objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this data security incident.

May 7, 2021
Page 2

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Will Daugherty". The signature is fluid and cursive, with a large, sweeping flourish at the end.

Will Daugherty
Partner

Enclosure



TRANSPORTATION
 Return Mail Processing Center
 P.O. Box 6336
 Portland, OR 97228-6336

<<Mail ID>>
 <<Name 1>>
 <<Name 2>>
 <<Address 1>>
 <<Address 2>>
 <<Address 3>>
 <<Address 4>> <<Date>>
 <<Address 5>>
 <<City>><<State>><<Zip>>
 <<Country>>

Notice of Data Security Incident

Dear <<Name 1>>:

ATC Transportation takes the privacy and security of personal information very seriously. We are writing to let you know about a data security incident we recently identified and addressed that may have involved some of your personal information. This notice explains the incident, the measures we have taken in response, and the steps you may consider taking to help protect your information.

What Happened?

On March 22, 2021, ATC Transportation discovered that it was the target of a ransomware attack in which an unauthorized actor used malware to encrypt certain servers. In response, we immediately took steps to secure our systems, launched an investigation, and engaged a leading cybersecurity firm to assist. Federal law enforcement was notified as well. Our investigation determined that the unauthorized actor gained access to certain systems within our environment at various times from approximately March 4, 2021 to March 22, 2021. During this time period, the unauthorized actor appears to have obtained some data from our systems.

What Information Was Involved?

On April 15, 2021, we learned the data potentially obtained by the unauthorized actor may have contained some of your personal information, including your name, <<data elements>>.

What Are We Doing?

To help prevent a similar incident from occurring in the future, we implemented additional security measures designed to enhance the security of our network, systems, and data. Additionally, we continue to support federal law enforcement’s investigation.

What You Can Do

We wanted to make you aware of the incident and provide you with additional information on steps you may consider taking. As a precaution, we have arranged for you to enroll, at no cost to you, in online, three-bureau credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. For more information on *myTrueIdentity*, including instructions on how to activate your complimentary one-year membership, as well as additional steps you may take to help protect your information, please see the additional information provided in the following pages.

For More Information

The security of your personal information is important to us and we sincerely regret that this incident occurred. If you have any questions, please call 855-654-0938, Monday through Friday, between 8:00 a.m. and 8:00 p.m. Central Time.

Sincerely,

A handwritten signature in black ink that reads "Brian Varano". The signature is written in a cursive style with a large initial "B".

Brian Varano
ATC Transportation

Complimentary One-Year *myTrueIdentity* 3B Credit Monitoring Service

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

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Insert Unique 12-letter 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, three-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 six-digit telephone passcode <<Insert static six-digit Telephone Pass Code>> 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.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. 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 a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily three-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, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

ADDITIONAL STEPS YOU CAN TAKE

Free Credit Report. Regardless of whether you choose to take advantage of the complimentary identity monitoring, it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. You may obtain information from the credit reporting agencies and the FTC about security freezes.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, <https://oag.dc.gov>, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.