BakerHostetler

Baker&Hostetler LLP
2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891
T 215.568.3100
F 215.568.3439
www.bakerlaw.com
Daniel A. Pepper
direct dial: 215.564.2456
dpepper@bakerlaw.com

June 11, 2020

VIA OVERNIGHT MAIL

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

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Tait Towers Manufacturing LLC ("TAIT"), a Pennsylvania manufacturing company that specializes in designing, constructing and delivering live event solutions, to provide a notice of a security incident.[1]

On June 5, 2020, TAIT concluded its investigation of a data security incident that involved unauthorized access to TAIT's computer server and the email accounts of certain TAIT personnel. Upon suspecting potential unauthorized access on April 6, 2020, TAIT took its servers and IT systems offline and launched an investigation with the assistance of a leading cyber security firm.

As part of the investigation, TAIT conducted a comprehensive review of the servers and email accounts to identify individuals whose information may have been involved in this incident. TAIT completed that review on June 5, 2020 and learned that unauthorized parties gained access to its network on February 16, 2020, through which they were able to obtain administrative account credentials to login to a server. The investigation was unable to rule out the possibility that the unauthorized party may have been able to access names, addresses, email addresses, dates of birth, Social Security numbers and financial account numbers.

Beginning on June 11, 2020, TAIT will mail notification letters via email to the New Hampshire residents whose information may have been involved in this incident, in accordance with N.H. Rev. Stat. Ann. § 359-C:20. A copy of the notification letter is enclosed. TAIT is offering one

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

year of complimentary credit monitoring and identity theft protection service through Experian to the individuals whose information may have appeared in the accessed accounts. TAIT is also providing a call center for the individuals to call with questions regarding the incident.

To help prevent a similar incident from occurring in the future, TAIT conducted a review of its cybersecurity defenses and protocols and has implemented additional safeguards, such as adding multi-factor authentication and deploying endpoint monitoring systems.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Daniel A. Pepper
Partner

Enclosure

TAIT

June 11, 2020

NOTICE OF DATA BREACH

Dear Sir or Madam:

Tait Towers Manufacturing LLC ("TAIT") takes data security very seriously and we understand the importance of protecting the information we maintain. We are writing to inform you about an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

WHAT HAPPENED: On April 6, 2020, TAIT became aware of a data security incident in which an unauthorized party accessed a TAIT computer server and the email accounts of certain TAIT personnel. Upon learning of the incident, TAIT immediately took its servers and IT systems offline and a leading cyber security firm was engaged to assist with the investigation. Although the investigation is ongoing, the investigation has revealed that the unauthorized access began on February 16, 2020.

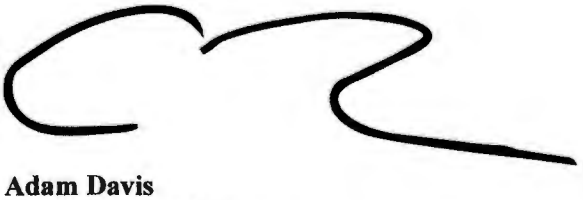
WHAT INFORMATION WAS INVOLVED: TAIT's investigation into this matter is ongoing, but TAIT has determined that the server content and email accounts accessed by the unauthorized party may have contained some individuals' names, addresses, email addresses, dates of birth, Social Security numbers or financial account numbers.

WHAT YOU CAN DO: To date, TAIT has no reason to believe that any of the information maintained in the server and email accounts was misused. Out of an abundance of caution, we encourage you to remain vigilant by reviewing your financial account statements for any unauthorized activity. If you see charges or activity you did not authorize, we suggest that you contact your financial institution immediately. As a precaution, we are prepared to offer credit monitoring at no charge to those individuals potentially affected by this incident. For more information or to sign up for credit monitoring, please call our dedicated call center for this issue at 855-917-3540.

WHAT WE ARE DOING: TAIT regrets any inconvenience or concern this may cause. We have taken steps to help prevent a similar incident from occurring in the future, such as adding multi-factor authentication and deploying endpoint monitoring systems, as well as additional actions to further expand and strengthen our security processes.

FOR MORE INFORMATION: For any questions you may have regarding this data security incident, please call our dedicated call center for this issue at 855-917-3540 Monday through Friday, from 9:00 a.m. to 9:00 p.m., Eastern Time.

Sincerely,



Adam Davis
Chief Creative Officer

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and credit reports for any unauthorized activity. 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, visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also contact the three nationwide credit reporting companies below:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You may also consider contacting your local law enforcement authorities and filing a police report. You may be asked to provide a copy of the police report to creditors to correct your records. Contact information for the Federal Trade Commission is below:

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

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. 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 reporting companies (Equifax, Experian, or Trans Union). A fraud alert is free. The credit reporting company you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit reporting companies will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting companies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You will need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit reporting company will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit reporting company to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit reporting company must lift a freeze within one hour. If the request is made by mail, then the reporting company must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift of the freeze because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit reporting companies.

Connecticut: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland: You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New York: You may contact and obtain information from these state agencies:

- 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
- New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit reporting companies and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. 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.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.

- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Tait Towers Manufacturing LLC Identifies and Addresses Data Security Incident

LITITZ, PENNSYLVANIA JUNE 11, 2020 – Today, Tait Towers Manufacturing LLC ("TAIT"), a manufacturing company that specializes in designing, constructing and delivering live event solutions, announced that it has identified and addressed a data security incident.

On April 6, 2020, TAIT became aware of a data security incident in which an unauthorized party accessed a TAIT computer server and the email accounts of certain TAIT personnel. Upon learning of the incident, TAIT immediately took its servers and IT systems offline and a leading cybersecurity firm was engaged to assist with the investigation. Although the investigation is ongoing, the investigation has revealed that the unauthorized access began on February 16, 2020. TAIT has addressed the security issues resulting in this incident, taking steps such as resetting the login credentials for TAIT's servers and email system. Additionally, TAIT conducted a review of its cybersecurity defenses and protocols and has implemented additional safeguards, such as adding multi-factor authentication and deploying endpoint monitoring systems.

To date, TAIT has no reason to believe that any of the information maintained in the server and email accounts was misused. TAIT is in the process of informing those individuals potentially affected so they can monitor for any suspicious activity. TAIT's investigation into this matter is ongoing, but TAIT has determined that the server content and email accounts accessed by the unauthorized party may have contained some individuals' names, addresses, email addresses, dates of birth, Social Security numbers or financial account numbers. Out of an abundance of caution, TAIT encourages its clients, employees and vendors to remain vigilant by reviewing their financial account statements for any unauthorized activity. As a precaution, TAIT is prepared to offer credit monitoring at no charge to those individuals potentially affected by this incident. For more information or to sign up for credit monitoring, please call our dedicated call center for this issue at 855-917-3540.

"TAIT takes data security very seriously and understands the importance of protecting the information it maintains," said Adam Davis, Chief Creative Officer at TAIT. "We are working to address this issue and regret any inconvenience this may cause to our valued employees, clients and vendors."

Additional information is available at www.taittowers.com/DataSecurityIncident or by contacting Kierston Powell via email at kierston.powell@taittowers.com or telephone at 717-606-4659.