Baker McKenzie LLP
300 East Randolph St.
Ste. 5000
Chicago, IL 60601
United States
Tel: +1 312.861.8000
www.bakermckenzie.com

February 17, 2023

VIA EMAIL
New Hampshire Attorney General
attorneygeneral@doj.nh.gov

RE: Data Breach Reporting

Dear New Hampshire Attorney General:

I am writing on behalf of Tom James Company ("Tom James") to notify you of a recent data security incident. Specifically, Tom James was the victim of a ransomware incident, which occurred on or around August 2022. In response to this incident, Tom James engaged a leading third-party cybersecurity forensics firm to first help ensure the system's security and integrity was restored, and to determine the scope of the incident. In the course of the investigation, Tom James determined that a limited number of files may have been subject to unauthorized access and acquisition.

Tom James is taking steps to protect the affected individuals following this incident. Following a thorough investigation with the assistance of its third-party partners, Tom James confirmed that personal information relating to approximately 8,656 individuals was included in the files that may have been subject to unauthorized access and acquisition, approximately 12 of whom are New Hampshire residents. The potentially-impacted personal information for some individuals included name and Social Security number.

Tom James is providing notice to all potentially-affected individuals. Notice to these individuals who are residents of New Hampshire will be sent on or about February 17, 2023 by postal mail. A copy of this notice is attached. These individuals are also being provided 12 months of credit monitoring services through Experian, at no cost to them.

Please feel free to contact me with any questions at

Regards,

Nicholas Merker
Partner

TOM JAMES
SINCE 1966

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 17, 2023

J0440-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 DOMESTIC 1 YEAR
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

RE: Notice of Data Breach

Dear Sample A. Sample:

We value our relationship with you and respect the privacy of your information, which is why, as a precautionary measure, we are writing to notify you of a recent incident that may affect the privacy of some of your personal information.

As you may know, we experienced a ransomware incident in August 2022 which caused issues and interruption to our IT systems. In partnership with several specialist consultants, we have conducted an exhaustive and very detailed investigation into the complex causes, the process and nature of the incident itself, and resulting impacts.

We write to provide you with information about the event, our response and steps taken to mitigate the effects of this incident (including to prevent this happening again), and steps you can take to protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? In August 2022, we discovered suspicious activity associated with certain portions of our network that we later identified as a ransomware attack. Immediately in response, we took steps to secure our network and began an investigation to determine the nature and scope of the activity. In addition to the availability and productivity issues experienced during this event, our investigation revealed that an unauthorized actor claimed to have accessed and/or acquired certain files from our environment during this event. As a result of this claim, we immediately undertook a comprehensive review of the potentially-impacted data to identify the information that may have been accessed during this event and to whom it related for purposes of notification. We thereafter worked to determine the residency of any potentially-impacted individuals as quickly as possible. We recently concluded this review. We are notifying you now because your information was present in one of the specific files involved in our review, and therefore may have been accessed during this event.

What Information Was Involved? Our investigation determined that the information related to you that may have been affected includes your name and Social Security number. While we have no evidence that any of your information was used for identity theft or fraud, we are notifying you out of an abundance of caution and providing information and resources to assist you protecting your personal information, should you feel it appropriate to do so.

What We Are Doing. We take this incident and the obligation to safeguard the information in our care very seriously. After discovering suspicious activity, we promptly responded, taking steps to confirm our network security, and conducting a comprehensive investigation of the event to determine its nature, scope, and impact. We also reported this event to federal law enforcement. Further, as part of our ongoing commitment to the privacy and security of personal information in our care, we are reviewing and enhancing our existing policies and procedures relating to data protection and security. We will also institute additional security measures, and

provide additional training to employees, to better protect against future incidents. We are also notifying relevant regulatory authorities, as required.

As an added precaution, we are offering you access to credit monitoring and identity theft protection services for twelve (12) months through Experian at no cost to you. If you wish to activate these services, you may follow the instructions included below. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by May 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted] by May 31, 2023. Be prepared to provide engagement number [redacted] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*****
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

What You Can Do. The data elements at issue in this event may create a risk of identity theft. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring your free credit reports for suspicious activity and to detect errors. You should report any such activity to law enforcement. You can also enroll to receive the complimentary credit monitoring services that we are offering to you. Please also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*.

For More Information. We understand that you may have questions that are not addressed in this notice, and we will, of course, assist with any queries or concerns you may have about this incident. If you have additional questions or concerns, you may call our dedicated data event call center at [redacted], which is available from 6:00 AM to 8:00 PM Pacific Time Monday through Friday, or from 8:00 AM to 5:00 PM Saturday and Sunday (excluding major U.S. holidays). Be prepared to provide your engagement number [redacted].

We appreciate how concerning this matter may be for you. You can be assured that this incident is a priority for us.

Sincerely,

Tom James Company

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

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	1-800-916-8800
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. If you are a non-US resident, you may also contact your national Data Protection Authority or law enforcement to report the incident and/or seek advice on how to mitigate any negative consequences of the incident. This notice has not been delayed by law enforcement.

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. Tom James Company is located at 263 Seaboard Lane Franklin, TN 37067.

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 to 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 5 Rhode Island residents impacted by this incident.