Buffalo
New York
Washington D.C.

www.octillolaw.com

August 18, 2023

VIA ONLINE SUBMISSION

Maine Office of the Attorney General
6 State House Station
Augusta, ME 04333

Office of the Attorney General:

On behalf of Milliman, Inc., ("Milliman"), whose office is located at 1301 5th Avenue, Suite 3800, Seattle, WA 98101, and pursuant to 10 Me. Rev. Stat. § 1346, *et seq.*, this letter provides notice of a recent data security incident. This letter is also submitted on behalf of Milliman's client, Trane Technologies. By providing this notice, Milliman does not waive any rights or defenses regarding the applicability of Maine law or personal jurisdiction.

Milliman provides administrative services to employee benefit and pension plan sponsors, including Trane Technologies. As part of those services, Milliman utilizes a third-party vendor, Pension Benefit Information, LLC ("PBI"), to conduct research on whether plan members and beneficiaries have passed away. For that purpose, Milliman transferred data regarding Trane Technologies' plan members to PBI utilizing a secure and encrypted file transfer protocol.

PBI recently notified Milliman that PBI experienced a data security incident affecting the data of Milliman's clients. Specifically, PBI disclosed that it utilized the "MOVEit Transfer" software provided by Progress Software Corporation ("Progress Software") for PBI's secure file transfer protocol ("SFTP") servers. PBI also indicated that it stored Milliman clients' data on PBI's SFTP servers utilizing the MOVEit Transfer software.

According to information provided to Milliman by PBI, on or around May 31, 2023, Progress Software disclosed for the first time that its MOVEit Transfer software contained a previously unknown, "zero-day" vulnerability that could be exploited by an unauthorized actor (CVE-2023-34362). PBI also disclosed that it launched an investigation into the nature and scope of the MOVEit vulnerability's impact to PBI's systems. According to PBI, its investigation determined that an unauthorized third party accessed one of PBI's MOVEit Transfer servers on May 29, 2023, and May 30, 2023, and downloaded data. PBI explained it then conducted a manual review of its data to confirm the identities of individuals potentially affected by this event. PBI completed that review on July 21, 2023, and confirmed to Milliman at that time that the personal information of certain plan members of Milliman's client Trane Technologies were affected and Milliman, following reconciliation of the data, was able to recently inform Trane Technologies of the scope of individuals whose information may have been affected.

PBI has advised us that it immediately took steps to patch the vulnerability in its MOVEit Transfer software, and PBI is reviewing and enhancing its information security policies and procedures.

Milliman has stopped transferring data to PBI pending further evaluation of PBI's information security practices. Milliman is also evaluating potential vendor management and security enhancements.

Together with PBI, Milliman has determined that the incident involved the personal information of eight (8) Maine residents as it relates to Trane Technologies. While the specific personal information varies by individual, the categories of information included, but were limited to, names, social security numbers, dates of birth, and mailing addresses. PBI is providing written notification to those individuals on behalf of Milliman and Trane Technologies, which includes an offer for twenty-four (24) months of cost-free credit monitoring. This notification will be sent to the impacted Maine residents via regular mail starting on August 18, 2023. A sample copy of that individual notice is attached for your review.

Please feel free to contact me with any questions at (716) 898-2102 or dgreene@octillolaw.com.

Sincerely,

OCTILLO

Daniel P. Greene, Esq.
Certified Information Privacy Professional, United States (CIPP/US)
Certified Information Privacy Professional, Europe (CIPP/E)

Encl.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_3 (variable header)>>

Dear <<first_name>> <<last_name>>:

Pension Benefit Information, LLC ("PBI") provides audit and address research services for insurance companies, pension funds, and other organizations, including pension plans sponsored by Trane Technologies Company LLC or its affiliates. PBI is providing notice of a third-party software event that may affect the security of some of your information. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review on July 21, 2023, and confirmed that information concerning a limited number of Trane Technologies pension plan members was among the records involved in this incident.

What Information Was Involved? Our investigation determined that the following types of information related to you were present in the server at the time of the event: <<b2b_text_2 (full name and Data Elements)>>.

What We Are Doing. We take this event and the security of information in our care seriously. Upon learning about this vulnerability, we promptly took steps to patch servers, investigate, assess the security of our systems, and notify potentially affected customers and individuals associated with those customers. In response to this event, we are also reviewing and enhancing our information security policies and procedures.

While we are unaware of any identity theft or fraud as a result of this event, as an additional precaution, PBI is offering you access to 24 months of complimentary credit monitoring and identity restoration services through Kroll. Details of this offer and instructions on how to activate these services are enclosed with this letter.

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. Please also review the enclosed *Other Important Information*, which contains information on what you can do to safeguard against possible misuse of your information. You can also enroll in the credit monitoring services that we are offering.

For More Information. If you have additional questions, you may call our toll-free assistance line at TFN Monday through Friday from 9:00 am to 6:30 pm Eastern time (excluding U.S. holidays). You may also write to PBI at 333 South Seventh Street, Suite 2400, Minneapolis, MN 55402.

Sincerely,

The PBI Team

Other Important Information

Enroll in Kroll's Monitoring Services

To help relieve concerns and restore confidence following this event, we have secured the services of Kroll to provide identity monitoring at no cost to you for 24 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.[1]

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (Activation Date)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional Information

- **Credit Monitoring**. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.
- **Fraud Consultation**. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.
- **Identity Theft Restoration**. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 one-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

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

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 they are a victim of identity theft.

Should consumers wish to place a security freeze or fraud alert, 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
1-888-298-0045	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 Security Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Security Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Security Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, security freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For California Residents, you may also wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.

For District of Columbia residents, you may also obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Iowa Residents, you are advised to report suspected incidents of identity theft to law enforcement or the Iowa Attorney General's Office at Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, telephone: 1-515-281-5926 or 1-888-777-4590.

For Maryland residents, you may obtain information about avoiding identity theft from the Maryland Office of the Attorney General at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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, you may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General by calling 1-800-771-7755 or visiting https://ag.ny.gov; the New York State Police by calling 1-518-457-6721 or visiting https://troopers.ny.gov/; and/or the New York Department of State by calling 1-800-697-1220 or visiting https://www.dos.ny.gov.

For North Carolina residents, you may obtain additional information about preventing identity theft provided by the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon Residents, you are advised to report any suspected incidents of identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

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, individuals have the right to obtain any police report filed in regard to this event. <<b2b_text_4 (There are approximately [Number] Rhode Island residents that may be impacted by this event.)>>