

August 14, 2023

VIA EMAIL

Idaho Attorney General's Office
Consumer Protection Division
700 W. Jefferson Street
P.O. Box 83720
Boise, ID 83720-0010
Email: agwasden@ag.idaho.gov

Dear Sir or Madam:

On behalf of Milliman, Inc., (“Milliman”), and pursuant to Idaho Code § 28-51-104 *et seq.*, this letter provides notice of a recent data security incident. This letter is also submitted on behalf of certain Milliman clients identified in the attached Appendix A. By providing this notice, Milliman does not waive any rights or defenses regarding the applicability of Idaho law or personal jurisdiction.

Milliman provides administrative services to employee benefit and pension plan sponsors. 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 its clients’ consumers 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 consumers of Milliman’s clients were affected and

Milliman, following reconciliation of the data, was able to recently inform its clients of the scope of individuals whose information may have been affected.

The Milliman clients whose consumer data was affected by the incident include those companies listed in the attached Appendix A.

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 869 Idaho residents. While the specific personal information varies by individual, the categories of information included, but were limited to, names, addresses, dates of birth, and social security numbers. PBI is providing written notification to those individuals on behalf of Milliman and its clients identified herein, which includes an offer for 24 months of cost-free credit monitoring. This notification will be sent to the impacted Idaho residents via regular mail starting on August 14, 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

A handwritten signature in black ink, appearing to read 'D. Greene', with a stylized flourish extending to the right.

Daniel P. Greene, Esq.

Certified Information Privacy Professional, United States (CIPP/US)

Certified Information Privacy Professional, Europe (CIPP/E)

Encl.

APPENDIX A
Milliman Impacted Client List

Acuity Brands Lighting, Inc.
AdventHealth
AECOM
Aflac Incorporated
AGFA Corporation
Albemarle Corporation
Allen & Company LLC
Alliance Beverage Distributing Co.
Alpha Metallurgical Resources
Altec, Inc.
Amentum
American Cancer Society
American Society of Composers, Authors and Publishers
Amtrak
Antelope Valley Medical Center
Apple Bank for Savings
Aramco
Archdiocese of Galveston-Houston
Archdiocese of Portland in Oregon
Argo Group US, Inc.
Armstrong County Memorial Hospital
ASARCO, LLC
Atalco LLC
Atrium Health
Babcock Power Inc.
Baptist Health
Barton Group
Bi-State Development Agency of the Missouri-Illinois Metropolitan District
Blue Bird Corporation
Blythedale Children's Hospital
Board of Trustees of the Prosecuting Attorneys' and Circuit Attorneys' Retirement System
Boise Cascade Company
Bose Corporation
Brighthouse Financial
Brooklyn Bureau Of Community Service
Broward Health
California School Employees Association
Cal-Oak Products
Carl Zeiss, Inc.
Cascade Hardwoods
Case Western Reserve University
Casio America
Catholic Church Extension Society
Catholic Diocese of Fort Worth
CCX, Inc.
CEMEX, Inc.
CH2MHill BWXT West Valley, LLC
Chart Industries, Inc.
City of Oxnard
City of San Clemente
Clearwater Paper Corporation
Collins Pine
Columbian Mutual Life Insurance Company

Community Service Society of New York
Conagra Brands, Inc.
Concord Hospital - Laconia
Consumer Portfolio Services
Continental Divide Electric Cooperative
Cotter Corporation
CoxHealth
Credit Human Federal Credit Union
CRH Americas
Dallas Theological Seminary
Delta Health System
Dolese Bros. Co.
Donnelley Financial US, LLC
East Cambridge Savings Bank
Elliot Health System
Equitable Financial Life Insurance Company
Erste Group Bank AG New York Branch
Finch Paper LLC
First Financial Bancorp
Firstmark Credit Union
Fish & Richardson P.C.
Frontier Communications Parent, Inc.
Fulton County Medical Center
General Atomics and Affiliated Companies
Golden Rain Foundation of Walnut Creek
Good Samaritan Hospital Corvallis
Gorton's Inc.
Graco Inc.
Grand View Health
Gränges Americas Inc.
Guard Publishing Company
Hawai'i Pacific Health
Haworth Inc.
Helena Agri-Enterprises, LLC
Hopkes Logging Company
Hospital Central Services Cooperative, Inc.
IMT Insurance Company
Ingersoll Rand Industrials
Intercounty Electric Cooperative Association
J.R. Simplot Company
Japan Airlines International Co., Ltd.
Jewish Federation Council of Greater Los Angeles
Kaiser Permanente
Kayser-Roth Corporation
Kearney-National Inc.
Keeneland Association, Inc.
Kern Regional Center
King Ranch, Inc.
Kloeckner Namasco Holding Corporation
Knights of Columbus
L.A. Philharmonic Association
Lenawee County
Lighthouse Guild International, Inc.
LSC Communications LLC
Lutheran Social Service of MN
Macy's Department Stores

Magellan Midstream Partners, LP
Maimonides Medical Center
Marshall Medical Center
Maxar
Medical Insurance Exchange of California
Memorial Health System
Merle Norman Cosmetics, Inc.
Merrill & Ring Inc.
Metropolitan Transit Authority of Harris County
Miller & Chevalier Chartered
Modesto Irrigation District
Motion Picture Association, Inc.
Motiva Enterprises LLC
MultiCare Health System
Munich American Reassurance Company
Municipal Employees Credit Union Of Baltimore, Inc.
Murphy Company
Nabors Industries
Narragansett Bay Commission
National Geographic Society
Noble Services Company LLC
North Dakota Farmers Union
North Shore Bank
Northeast Georgia Health System, Inc.
Northeast Medical Center Hospital
Northwest Fiber, LLC dba Ziplly Fiber
Novus International, Inc.
NY Daily News Enterprises, LLC
Office Depot OfficeMax
Olympus Corporation of the Americas
Optimus Steel, LLC
Packaging Corporation of America
Parkland Health and Hospital System
Pedernales Electric Cooperative, Inc.
PeoplesBank
Petroleum Club of Houston
Pioneer North America, Inc.
Piper Aircraft, Inc.
PNM Resources, Inc.
PotlatchDeltic Corporation
Providence Health & Services
Puget Sound Energy
Qualstar Credit Union
Rayonier Advanced Materials Inc.
Rayonier Inc.
Renasant Bank
Burger King Company, LLC
Ripley Entertainment, Inc.
Robinson Industries, Inc
Rockefeller Group
Royal Neighbors of America
R.R. Donnelley & Sons Company
RSG
Salado Isolation Mining Contractors, LLC
San Diego Union-Tribune
San Jacinto River Authority

SantaFe HealthCare, Inc. (AvMed, Inc.)
Savings Bank Of Danbury
SCO Family of Services
Sekisui America Corporation
Senior Operations LLC
Sheet Metal Workers Local No. 124
Simpson / Green Diamond
South Dakota Farmers Union
South Jersey Industries
Southern Minnesota Beet Sugar Cooperative
Southern New Hampshire Medical Center
Stimson Lumber Company
Sumitomo Mitsui Banking Corporation
Swanson Group
SWIFT
Symrise Inc.
Taylor Morrison, Inc.
Teck American
Tenet Healthcare
Texans Credit Union
Texas Scottish Rite Hospital for Children
The California Endowment
The New York Racing Association, Inc.
The Oklahoma Publishing Company
Thomaston Savings Bank
Thryv Holdings, Inc.
TidalHealth Nanticoke, Inc.
Tidewater Inc.
Titan International, Inc.
Town of Brookfield
Town of Greenwich
TriMas
Truman Medical Centers
UniSea, Inc
United Jewish Appeal-Federation of Jewish Philanthropies of NY Inc & Affiliated Agencies
University of Missouri System
Utah Transit Authority
Vanderbilt Minerals, LLC
Vigilant
Vigor Industrial
Virginia Mason Medical Center
Vizient, Inc.
Volunteer Energy Cooperative
Volunteers of America
Walton Electric Membership Corporation
Washington Mills Tonawanda, Inc.
West Georgia Health System
Windstream Services, LLC
Woodward, Inc.
WorldVision, Inc.
XL America, Inc.
Yakima Valley Medical
Yamhill Log Scaling & Grading



<<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(Notice of Data Breach)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Pension Benefit Information, LLC (“PBI”) provides audit and address research services for insurance companies, pension funds, and other organizations<<b2b_text_1(“, including” data owner)>>. 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.

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(name, 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 for the next twelve to twenty-four months and to report suspected identity theft incidents to the institution. Please also review the enclosed *Steps You Can Take to Help Protect Personal 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](tel:1-800-368-7777), Monday through Friday from 9:00 a.m. to 6:30 p.m. 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

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL 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 deadline)>> 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 “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 a consumer’s name without consent. However, consumers should be aware that using a credit 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 credit freeze on their credit report. To request a credit 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;
5. Proof of current address, such as a current utility bill or telephone bill;

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.

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 credit 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 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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 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 <https://www.marylandattorneygeneral.gov/>.

For Massachusetts residents, you have the right to obtain any police report filed in regard to this event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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, 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, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. <<b2b_text_4(For certain PBI clients, there are approximately [#] Rhode Island residents that may be impacted by this event.)>>