



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

June 22, 2023

J5981-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 ADULT
 APT ABC
 123 ANY STREET
 ANYTOWN, ST 12345-6789



Re: Notice of Data Breach

Sample A. Sample,

We are writing to inform you about a recent cybersecurity breach at our third-party provider, PBI Research Services/Berwyn Group (“PBI”) involving the MOVEit Transfer application, which is used by thousands of organizations worldwide. CalPERS uses PBI’s services to ensure accuracy in its payments to retirees and beneficiaries. The cybersecurity breach did not impact CalPERS’ information systems or our member benefits website, myCalPERS.

The cybersecurity breach involves your personal information. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing, as well as information on how you can obtain free credit monitoring.

What happened?

PBI provides services to CalPERS to identify member deaths. This ensures that proper payments are made to retirees and beneficiaries and prevents instances of overpayments or other errors.

CalPERS provided data to PBI in a secure, encrypted format. On June 6, 2023, PBI notified CalPERS that a previously unknown "zero-day" vulnerability in the MOVEit transfer application allowed our data to be downloaded by an unauthorized third party.

What personal information was involved?

Your personal information that was downloaded included: [Extra1]. [Extra2]

What we are doing:

CalPERS took immediate steps to enhance the security of its members’ benefits. This includes new protocols on myCalPERS, as well as additional safeguards for those who use the member call center or visit any CalPERS regional office.

In addition, CalPERS is offering you a complimentary 24-month membership of Experian’s® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: September 30, 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: ABCDEFGHI**

0000001



What you can do:

In addition to enrolling in the credit monitoring being offered to you, we encourage you to take the following precautions:

- It is always a good idea to remain vigilant against threats of identity theft or fraud and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.
- If you ever suspect that you are the victim of identity theft or fraud, you can contact your local police. Additional information about how to protect your identity is contained in this mailing.

For more information:

CalPERS has set up a dedicated page on its website if you have additional questions. Members can visit calpers.ca.gov/PBI or email their questions to PBIquestions@calpers.ca.gov. You can also call the dedicated call center toll free Monday through Friday 6am – 8pm PT, or Saturday and Sunday from 8am – 5pm PT (excluding major U.S. holidays) at 833-919-4735.

We regret having to inform you of PBI's security breach. We take the security of our data very seriously and will continue to take precautions to protect you in the future.

Sincerely,

Marcie Frost

Chief Executive Officer

ADDITIONAL DETAILS REGARDING YOUR 24-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 agents 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.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (833) 919-4735. 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 (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 this Identity Restoration support is available to you for 24 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. You will also find self-help tips and information about identity protection at this site.



MORE INFORMATION ABOUT IDENTITY PROTECTION

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax	Experian	TransUnion
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
(888) 766-0008	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

District of Columbia Residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov, and www.oag.dc.gov.

California Residents: Visit the California Office of Privacy Protection (<https://oag.ca.gov/privacy>) for additional information on protection against identity theft.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, +1 (515) 281-5164, www.iowaattorneygeneral.gov.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the cybersecurity 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.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-566-7226 (Toll-free within North Carolina); +1 (919) 716-6400; or www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341, +1 (800)-771-7755; or www.ag.ny.gov.

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, +1 (877) 877-9392 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us.

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903; +1 (401) 274-4400; or www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, Washington, D.C., and West Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).



FREQUENTLY ASKED QUESTIONS

What happened?

CalPERS was informed about a recent cybersecurity breach at our third-party vendor PBI Research Services/Berwyn Group (“PBI”) involving their MOVEit Transfer Application, which is used by thousands of organizations worldwide. CalPERS uses PBI’s services to ensure accuracy in its payments to retirees and beneficiaries and sent data to PBI in a secure, encrypted format.

The cybersecurity breach did not impact CalPERS’ information systems or myCalPERS.

Specifically, PBI provides services to CalPERS to identify member deaths. These services ensure that proper payments are made to retirees and beneficiaries and prevent instances of overpayments or other errors. PBI also validates information on inactive members who may soon be eligible for benefits.

On June 6, 2023, PBI notified CalPERS that a previously unknown “zero-day” vulnerability in their MOVEit Transfer Application allowed our data to be downloaded by an unauthorized third party.

PBI has reported the matter to federal law enforcement and has told CalPERS it has resolved the vulnerability, while also adding additional security measures.

What personal information was involved?

Personal information that was downloaded included: First and Last Name; Date of Birth; and Social Security Number. It could have also included the names of former or current employers, spouse or domestic partner, and child or children.

What is CalPERS doing to protect its members?

CalPERS took immediate steps to enhance the security of its members’ benefits. This includes new protocols on the member benefits website, myCalPERS, as well as additional safeguards for those who use the member call center or visit any CalPERS regional office. CalPERS will also continue to thoroughly vet any security procedures of its vendors that receive retiree information.

CalPERS is offering all impacted members two years of complimentary credit monitoring and identity restoration services through Experian. If you have additional questions about protecting your personal information, please call the dedicated call center at 833-919-4735.

What can you do to protect yourself?

In addition to enrolling in the credit monitoring services, we encourage you to take the following precautions:

- Remain vigilant to threats of identity theft or fraud by regularly reviewing and monitoring your accounts and credit history for signs of unauthorized transactions or activity.
- If you ever suspect you are a victim of identity theft or fraud, you can contact your local police. Visit calpers.ca.gov/PBI for additional information on how to protect your identity.

Will this impact my monthly benefit payment?

No. CalPERS’ systems were not impacted. Your monthly pension payment will continue to be deposited to your bank account or mailed to you if you have chosen to receive a paper check.

Is my retirement money safe with CalPERS?

Yes. CalPERS’ systems were not impacted.

Does this effect all types of CalPERS retirees?

Yes. This includes retirees from the state, public agencies, school districts and retirees of the Judges’ Retirement System and Legislators’ Retirement System.

Does this impact active members of CalPERS?

No. This incident only involves information on CalPERS retirees and their survivors.

Can I continue to safely do business with CalPERS?

Yes. CalPERS systems were not impacted.

Was CalPERS the only organization impacted?

No. Thousands of organizations worldwide were also impacted.

Who can I call if I have additional questions?

You can receive information by calling the dedicated call center at 833-919-4735.