



THOMAS C. BILELLO
Vice President & Associate General Counsel
Office of General Counsel

February 18, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Dear Sir or Madam:

Pacific Life Insurance Company is writing to notify you of a data security incident involving one Maryland resident.

On Tuesday, December 14, 2021, an applicant reported that the online portal, where copies of policy documents are made available to applicants, displayed documents that did not belong to the applicant. In accordance with Pacific Life's procedures, an investigation was promptly opened to research the reported experience and to take appropriate corrective action.

On Thursday, December 16, 2021, Pacific Life determined that application forms related to one Maryland resident and collected as part of the application process were made accessible to other applicants. Those forms included: Application – Part I (containing addresses and contact information, tax identification number, income information, employment information, names of beneficiaries, coverage amounts, and type of coverage applied for, etc.); Application – Part II (containing medical information); HIPAA Authorization form; Replacement Notice; and the Electronic Delivery Consent Form.

Our investigation found that updates intended to add an additional layer of security were made to the portal's firewall. The updates introduced a caching feature that had unintended consequences. The documents of applicants who logged into the portal were cached for a limited time, making them accessible to other applicants who subsequently logged in within that timeframe. Pacific Life promptly terminated access to portal for all users on December 16. Since that time, additional controls to the underlying service have been added.

One Maryland resident has been identified as impacted by this incident. Notifications and credit monitoring are being provided to this individual. A copy of the draft notice is enclosed. Pacific Life has no indication that personal information related to this incident has been used for fraudulent purposes, or has resulted in identity theft, fraud or financial loss to the consumer.

For questions, or further information, please contact me at (949) 420-7078.

Very truly yours,

Thomas C. Bilello

Enclosure

PACIFIC LIFE INSURANCE COMPANY

700 Newport Center Drive, Newport Beach, California 92660-6397 Tel (949) 219-XXXX; Fax (949) 219-XXXX
www.PacificLife.com

January 21, 2022

Name
Address
City State Zip

Re: Notice of Data Breach

Dear

We are writing to inform you of a data privacy incident that may have involved your personal information. Pacific Life Insurance Company ("Pacific Life") takes the privacy of your information very seriously and we are sending you this letter to provide you with complimentary credit and identity monitoring services and to inform you about steps you can take to protect your information.

What Happened?

On Tuesday, December 14, 2021, an applicant reported that the online portal where copies of policy documents are made available to applicants, displayed documents that did not belong to the applicant. In accordance with Pacific Life's procedures, an investigation was promptly opened to research the reported experience and to take appropriate corrective action.

On Thursday, December 16, 2021, the investigation found that updates intended to add an additional layer of security were made to the portal's firewall. The updates introduced a caching feature that had unintended consequences. The documents of applicants who logged into the portal were cached for a limited period of time potentially exposing their documents to other applicants who subsequently logged in within that window of time.

What Information Was Involved?

The documents that may have been viewable on this site include forms that are collected as part of the application process. This can include: Application – Part I (includes addresses and contact information, tax identification number, income information, employment information, names of beneficiaries, coverage amounts and type of coverage applied for, etc.), Application – Part II (contains medical information), HIV Consent Form, HIPAA Authorization form, and Payment Authorization (contains bank information) as well as other forms required to issue a policy.

What We Are Doing.

Upon identification of the root cause on December 16, 2021, the portal was immediately shut down and the feature was disabled. Additional controls to the underlying service have been added as a second line of defense. In addition, to help prevent and detect any misuse of your information, we are offering you a complimentary two-year membership to "ReliaShield Elite". This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. Below are instructions for registering for ReliaShield.

Activate ReliaShield Now in Three Easy Steps:

1. Ensure you enroll by February 28, 2022
Activate membership by visiting Reliashield® Web Site:
<https://member.reliashield.com/enrollment/55>

- a. Please make sure this is the URL that is used as a different URL may make the codes unusable or create errors during enrollment.
2. Provide your activation code: PAC2MIK578Y
3. If you have questions or need an alternative to enrolling online, please call (888) 201-1944 or info@reliashield.com

What You Can Do.

We suggest that you follow the recommendations on the following page to protect your personal information. In addition, we recommend that you review your financial account statements and if you notice any suspicious activity, contact your financial institution. We also encourage you to contact ReliaShield to enroll in free identity and credit monitoring using the enclosed instructions.

For More Information: More information about how to protect your personal information appears on the following page.

If you have questions, you can contact also contact Pacific Life at 949-420-8412 from 8:00 a.m. Pacific until 5 p.m. Pacific, Monday through Friday.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Stephanie Babkow
Vice President New Buisness & Underwriting
Pacific Life Insurance Company

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 12 months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You are encouraged to report suspected identity theft to the FTC. You may also report suspected identity theft to local law enforcement, including the Attorney General in your state.

**Federal Trade
Commission**

600 Pennsylvania Ave,
NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Rhode Island

Attorney General
150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
401-274-4400

**Maryland Attorney
General**

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

**North Carolina
Attorney General**

9001 Mail Service
Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>