LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

February 17, 2020

File No. 34181.336

VIA WEB SUBMISSION

Xavier Becerra, Attorney General
Attorney General's Office
California Department of Justice
Attn: Public Inquiry Unit
P.O. Box 944255
Sacramento, CA 94244-2550

Re: Notice of Data Security Incident

Dear Attorney General Becerra:

We represent Pacific Guardian Life Insurance Co. Ltd. ("Pacific Guardian Life"), a domestic life and disability insurer located in Honolulu, Hawaii. This letter is being sent on behalf of Pacific Guardian Life because personal information belonging to California residents may have been affected by a recent data security incident. This information may have included unauthorized access to individuals' names, Social Security numbers, and, in very few cases, medical information.

On November 4, 2019, Pacific Guardian Life became aware of suspicious activity within the email account of one of its employees. It immediately took steps to secure the email account and began an internal investigation. In the course of the investigation, Pacific Guardian Life engaged a leading independent digital forensics firm to determine the nature and scope of the incident. On November 21, 2019, this investigation determined that an unauthorized individual obtained access to the employee email account, and may have viewed or downloaded emails from the account. Pacific Guardian Life then undertook to investigate the contents of the account that may have been impacted and determine whether protected personally identifiable information may have been involved. As a result of that investigation, Pacific Guardian Life confirmed that some individuals' personal information may have been in the email account and worked diligently to identify address information required to notify the potentially impacted individuals. On February 3, 2020, Pacific Guardian Life identified 1,214 California residents within the potentially affected population.

Pacific Guardian Life is not aware of any fraudulent activity as a result of this incident. Additionally, it will work with cybersecurity experts to independently review the security of its network and further enhance security levels as deemed necessary to minimize the likelihood of a similar event occurring in the future.

Pacific Guardian Life will be notifying the potentially affected California residents on or about February 18, 2020, via the attached consumer notification template. Out of an abundance of caution, Pacific Guardian Life is offering twelve (12) months of complimentary credit and identity monitoring services to the potentially affected residents.

Please contact me should you have any questions.

Very truly yours,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Attachment: California Consumer Notification Template

PACIFIC GUARDIAN LIFE
C/O ID Experts
PO Box 4219
Everett, WA 98204

To Enroll, Please Call:
1-833-554-0468
Or Visit:
https://ide.myidcare.com/pglife
Enrollment Code:
<<XXXXXXXX>>

F3245-2CA-0000002 P003 T00014 *********ALL FOR **** ###
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

February 18, 2020

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a data incident that may involve your personal information. Pacific Guardian Life Insurance Company, Limited ("Pacific Guardian Life") is committed to making sure you are able to take the necessary steps to protect your data so we are sending you this letter to inform you of this issue and provide you with complimentary credit and identity monitoring services.

What Happened? On November 4, 2019, Pacific Guardian Life became aware of suspicious activity within an employee's email account. We immediately took steps to secure the affected email account and began an internal investigation into the issue. We then engaged a leading independent digital forensics firm to help conduct the investigation and determine the nature and scope of the incident. On November 21, 2019, the investigation determined that there was unauthorized access to an employee email account, and that emails within that account may have been viewed or downloaded. Following a detailed analysis of the data in the employee's email account, on January 21, 2020, our investigation revealed that some of your personal information may have been contained within the affected email account. Since that time, we have been working diligently to identify contact information for the individuals potentially affected by this issue.

While there is no evidence to suggest any data potentially involved in this issue has been misused, we are sending you this letter to inform you of the incident and to share steps you can take to help protect your information, including enrolling in complimentary identity theft protection services.

What Information Was Involved? The information involved may have included your <<Variable Text>>.

What We Are Doing. As soon as we discovered the incident, we took immediate and active steps to address the issue. In addition, we have taken affirmative steps to minimize the likelihood of a similar incident occurring in the future. This includes working with leading cybersecurity experts to independently review the security of our network environment. We plan to take the findings of that review and use them to further enhance the security our network. As an added precaution, we are offering complimentary identity theft protection services through ID Experts®, a data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

0000002

What You Can Do. Follow the recommendations enclosed in this letter to help protect your personal information. Also, while there is no evidence to suggest any data potentially affected by this issue has been misused, we encourage you to enroll in the complimentary MyIDCare services through ID Experts by calling 1-833-554-0468 or going to https://ide.myidcare.com/pglife and using the Enrollment Code provided above. Please note the deadline to enroll is May 18, 2020. To activate credit monitoring you must be over the age of 18, and have established credit in the U.S., a Social Security number in your name, and a U.S. residential address associated with your credit file.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions, please call 1-833-554-0468 Monday through Friday from 6 am - 6 pm Pacific Time (4 am – 4 pm Hawaii Standard Time).

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

Sincerely,

Hisashi Matsuki
President and Chief Executive Officer
Pacific Guardian Life Insurance Company, Ltd.

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	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	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 fraud alerts, security freezes, and other 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	**Rhode Island**	**Maryland Attorney General**	**North Carolina Attorney General**
600 Pennsylvania Ave, NW	Attorney General	200 St. Paul Place	9001 Mail Service Center
Washington, DC 20580	150 South Main Street	Baltimore, MD 21202	Raleigh, NC 27699
consumer.ftc.gov, and	Providence, RI 02903	oag.state.md.us	ncdoj.gov
www.ftc.gov/idtheft	http://www.riag.ri.gov	1-888-743-0023	1-877-566-7226
1-877-438-4338	401-274-4400		

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.

0000002