Lombard International

One Liberty Place
1650 Market Street, 54th Floor
Philadelphia, PA 19103
United States of America

+1-484-530-4800 (Telephone)
+1-215-977-7820 (Fax)
www.lombardinternational.com

LOMBARD
INTERNATIONAL

July 17, 2023

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

Re: Data Breach Notification – Maryland

Dear Sir or Madam,

On Tuesday June 6, 2023, Lombard International Life Assurance Company ("LILAC") was advised by Pension Benefit Information Inc. (PBI) of Minneapolis, Minnesota, a third party service provider which provides services related to monitoring of death master file information that enable LILAC to identify the deaths of insureds under LILAC variable life insurance policies and variable annuity contracts, of a possible impact on information of LILAC contained in PBI's computer system.

PBI advised at the time that the unauthorized third party gained access to the information in question by exploiting a vulnerability in the MOVEit Transfer file transfer application used by PBI. PBI also advised that it was working with cybersecurity specialists to determine the scope of the unauthorized access and had also been in contact with federal law enforcement.

On June 21, 2023, PBI confirmed to LILAC that files containing LILAC information had in fact been accessed and copied by an unauthorized party. PBI also stated that it was continuing its investigation and had taken remedial measures to protect its system from the MOVEit Transfer vulnerability. No LILAC computer system was accessed without authorization or otherwise affected as part of the third party's unauthorized access to the PBI system.

The information accessed and copied by the unauthorized party includes the following information regarding insureds and/or annuitants under LILAC policies residing in Maryland:

Social Security Number
Last Name, First Name, Middle Name, Suffix
Date of birth
City, state and zip code of residence
Policy Number

LILAC has determined that there are 18 persons residing in Maryland affected by the unauthorized access to PBI's computer system.

After receiving notice of the breach by PBI, LILAC investigated the event and determined that it could not have prevented this cyber-incident, as it resulted entirely from the vulnerability in the MOVEit Transfer tool used by PBI to help it provide services to LILAC. LILAC has temporarily suspended providing further data to PBI until it can be assured that PBI has restored the security of its systems.

We are continuing to work with PBI to develop additional information regarding the unauthorized access to PBI's system. LILAC will be providing notification to the 18 affected persons residing in Maryland on July 19, 2023, a copy of the form of notification is attached to this letter.

Sincerely,

John Reilly
Executive Vice President & US General Counsel

[Date]

[Name]

[Address]

[City, State, ZIP]

Dear [Name]:

RE: NOTICE OF DATA BREACH

We are writing to inform you about an incident where an unauthorized third party acquired a copy of certain of your personal information. We deeply value our relationship with you and want to ensure peace of mind. Therefore, in this notice, we provide you with details about the situation and outline the steps you can take to help protect yourself.

WHAT HAPPENED?

On June 6, 2023, Lombard International Life Assurance Company ("Lombard") was advised by Pension Benefit Information, LLC ("PBI"), a third-party service provider to Lombard, that an unknown third party was believed to have gained unauthorized access to certain of PBI's data files by exploiting a vulnerability in the MOVEit Transfer software that PBI uses in file transfer activities.

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 its business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on its systems. Through the investigation, PBI learned that the third party accessed one of its MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. PBI 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. PBI recently completed that review.

On June 21, 2023, PBI confirmed definitively to Lombard that a number of files sent to PBI to support Lombard's administration of life insurance and annuity policies were accessed and copied and provided specific information on individuals whose personal information was accessed. Unfortunately, it has been determined that some of your personal information was among the data accessed without authorization.

WHAT INFORMATION WAS INVOLVED?

The information that the unauthorized third party accessed may include the insureds' or annuitants' name, city and state of residence, date of birth, social security number, and policy number. While information accessed for most insureds or annuitants included all of the foregoing types of data, the information relating to some insureds and annuitants did not include every type of data. Lombard has no evidence that any of your personal information has been used to commit identity fraud.

WHAT WE ARE DOING?

Lombard takes this incident extremely seriously. PBI has informed Lombard that after detecting unusual activity, PBI took immediate steps to identify and contain the intrusion, and reported the matter to law enforcement. PBI has been working with external cybersecurity experts and has implemented specific steps to safeguard against future unauthorized access to its systems and the Lombard files provided to PBI.

Upon receiving notification of the breach from PBI, Lombard immediately conducted its own investigation, concluding that the cyber incident was beyond its control and resulted from the vulnerability in the MOVEit Transfer tool used by PBI. As a precautionary measure, Lombard has temporarily suspended providing further data to PBI until we can be assured that PBI has restored the security of its systems. We are also evaluating additional measures to further enhance our protocols for the protection of your personal information and accounts, whether held internally at Lombard or provided to third party service providers as outlined in our Privacy Policy.

To assist you in protecting yourself against potential identity theft, PBI is offering you access for 12 months to 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 *Steps You Can Take to 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 PBI is offering.

FOR MORE INFORMATION

We want to emphasize our commitment to helping you protect your credit, identity, and personal information. We deeply regret this incident, which was beyond our control, and sincerely apologize for any concerns it may have caused you. If you have further questions relating this matter, please do not hesitate to contact us toll-free at [number], Monday-Friday between [times] Eastern time.

Sincerely,

Lombard International Life Assurance Company

KROLL

We have secured the services of Kroll to provide identity monitoring at no cost to you for one year. 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[1] include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

1. You must activate your identity monitoring services by **October 1, 2023**. Your Activation Code will not work after this date.
2. Visit **Enroll.krollmonitoring.com/redeem** to activate your identity monitoring services.
3. Provide Your Activation Code: **2YJK-ZEVD-WTWW-TWZ** and Your Verification ID: **SF-009849**

Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services[1] from Kroll:

Single Bureau 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 can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[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.

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 by reviewing 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 also should 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.

To file a complaint with the FTC, go to *www.ftc.gov/idtheft*, call 1-877-ID-THEFT (877-438-4338), or by writing to Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

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 *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 print a copy of the request form at *www.annualcreditreport.com/cra/requestformfinal.pdf*. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax (800) 685-1111 *www.equifax.com* P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 *www.experian.com* 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	TransUnion (800) 916-8800 *www.transunion.com* P.O. Box 6790 Fullerton, CA 92834

Fraud Alert
We recommend placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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 *www.annualcreditreport.com*.

Credit Report Monitoring
In addition, PBI has arranged with Kroll to provide you with credit monitoring for one year at no cost to you. Information on registering for this service is included.

Security Freeze
In some US states, you have the right to put a security freeze on your credit file. 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 on Identity Theft
You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit *www.ftc.gov/idtheft* or call 1-877-ID-THEFT (877-438-4338). If you become a victim of identity theft, you may wish to visit the FTC's *IdentiyTheft.gov* website for information on how to report and recover from identity theft.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at *www.oag.state.md.us/idtheft*, or by sending an email to idtheft@oag.statemd.us, calling 410-576-6491, or by writing to 200 St. Paul Place, Baltimore, MD 21202.