Lumico
family of insurance companies

Lumico Life Insurance Company
Elips Life Insurance Company
175 King Street, Armonk, NY 10504

August 1, 2023

BY EMAIL

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
consumer@ag.iowa.gov

To Whom It May Concern:

On behalf of Lumico Life Insurance Company (NAIC #73504) and Elips Life Insurance Company (NAIC #85561) (collectively, "the Companies"), which are both part of the Lumico family of insurance carriers, this letter provides notice pursuant to Iowa Code § 715C of a cybersecurity incident involving Iowa residents. By way of background, Lumico Life Insurance Company and Elips Life Insurance Company are for-profit insurance carriers and their principal place of business is 175 King Street, Armonk, NY 10504. Based on currently known information, the Companies believe approximately 3168 affected individuals reside in your jurisdiction.

On June 19, 2023, the Companies were informed by their third-party service provider, NTT Data Services ("NTT"), that NTT's own third-party service provider, Pension Benefit Information, Inc. ("PBI"), was affected by the MOVEit zero-day security vulnerability (the "PBI Incident"). NTT's principal place of business is 7950 Legacy Drive Suite 900 Plano, Texas 75024. At this time, NTT informed the Companies that, as a result of the PBI Incident, an unauthorized third party may have obtained a portion of the Companies' policyholder data. Through NTT, PBI provides the Companies with regulatory compliance and operational support services to determine whether certain policyholders are still living. The Companies' third-party administrators, like NTT, provide PBI with the Companies' policyholder data needed to perform these services.

As explained to the Companies by NTT, PBI discovered on June 2, 2023 that it had been a victim of the MOVEit zero-day vulnerability, which it detected and mitigated that same day. PBI promptly launched an investigation into the nature and scope of the incident with the assistance of third-party cybersecurity specialists, and reported the event to federal law enforcement on June 3, 2023. PBI's investigation revealed that an unknown actor accessed one of the MOVEit Transfer servers on May 29 and 30, 2023, and downloaded certain data from that system. To date, the Companies have no evidence that any downloaded personally identifiable information has been misused. The Companies are not taking efforts to recover the data and are unaware of any efforts by NTT or PBI to recover the data.

The data compromise occurred entirely on PBI's systems as a result of the MOVEit zero-day vulnerability. The Companies understand that they are two of many companies impacted by the PBI Incident and do not appear to have been specifically targeted. Additionally, the Companies have no reason to believe that the MOVEit zero-

day vulnerability impacted their own systems or network environments or that the information compromised is reasonably likely to pose a risk of material harm to the Companies' normal business operations.

After learning about the PBI Incident, the Companies activated their incident response protocols while awaiting further information from NTT and PBI. Given the nature of this third-party incident, the Companies have not conducted an internal review of their controls in response to this incident and have not filed a separate report with law enforcement.

On June 26, 2023, NTT shared with the Companies that the PBI Incident affected certain data files NTT had received from PBI. The Companies are continuing to analyze those data files and, on June 30, 2023, determined that the compromised data included certain policyholder names, address information, policy numbers, Social Security numbers, gender, and dates of birth. While the Companies' review of the relevant data is still ongoing, based on currently known information, the Companies believe that approximately 3168 Iowa residents were impacted.

As a result, the Companies are notifying your office as well as individuals whose information was impacted. The Companies are offering all impacted individuals 24 months of free one-bureau identity theft and credit monitoring services and provided notice to individuals on or about July 28, 2023 via U.S. Mail. The Companies will provide your office with any material updates if applicable. The notice to individuals was not delayed as a result of law enforcement. A sample notification letter to impacted individuals with the complimentary credit monitoring offer is attached to this notice.

The Companies take the protection of personal information seriously and are committed to answering any questions that your office may have. Please do not hesitate to contact me at (914) 828-2193 or Patricia_Kelley@swissre.com.

Respectfully yours,

Patricia Kelley

Senior Vice President, Head Compliance

Lumico
insurance made clear

Lumico Life Insurance Company
175 King Street, Armonk, NY, 10504

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (NOTICE OF [Variable Header])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

The Lumico Life Insurance Company is writing to let you know about a third-party software vulnerability that impacted 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 yourself.

What Happened? Progress Software disclosed that cyber criminals actively exploited a vulnerability in the MOVEit Transfer application. Because thousands of organizations use MOVEit to support secure file transfers, this incident has affected many companies around the world, including our third-party service provider NTT Data Services ("NTT"), and has been the subject of widespread media coverage.

On June 19, 2023, NTT informed us that, between May 29 and 30 of this year, an unauthorized third party exploited the vulnerability in the MOVEit application, which NTT's external vendor Pension Benefits Information, LLC ("PBI") uses, and may have acquired some of our policyholder information. For context, we provide NTT with policyholder data that it shares with PBI to perform regulatory compliance and operational support services for the benefit of our policies.

As explained to us by NTT, PBI completed the recommended patching and remediation steps to secure its systems on June 2 and has informed law enforcement of the incident. On June 30, our review of the data provided by NTT determined that the unauthorized third party in fact had acquired some of our policyholder information, as listed below.

The incident occurred entirely within PBI's systems, and we have no reason to believe that it impacted our own systems or network environment. As noted, we are also one of many companies affected by the incident, and we have no reason to believe that our policyholder data was specifically targeted.

What Information Was Involved? <<b2b_text_3 (RI Sentence)>> Based on our analysis, we believe the following types of information related to you were impacted:

- Contact information, including name;
- Gender;
- Social Security number;
- Date of birth;
- Address; and
- Policy numbers.

What We Are Doing. We take this event and the security of our policyholders' information seriously. Upon learning about this incident, we activated our incident response protocols and took prompt steps to ensure the ongoing security of our policyholder information.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. 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.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> 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.

Additionally, relevant state regulators and federal law enforcement authorities have been notified regarding this incident.

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 Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information, including filing or obtaining a police report. You can also activate in the identity monitoring services that we are offering through Kroll.

For More Information. If you have additional questions, you may call our toll-free assistance line at <Kroll Call Center Number>, Monday through Friday from 9:00 am to 6:30 pm Eastern time (excluding U.S. holidays). You may also write to us at customerservice@lumico.com.

Sincerely,

The Lumico Life Insurance Company Customer Service Team

Membership Number: <<Membership Number s_n>>
Enrollment Deadline: *<<b2b_text_6 (activation date)>>*

Steps You Can Take To Help Protect Personal Information

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 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.

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.

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;
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 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.