

RECEIVED

JUN 21 2021

CONSUMER PROTECTION



MULLEN  
COUGHLIN<sub>LLC</sub>  
ATTORNEYS AT LAW

Julie Siebert-Johnson  
Office: (267) 930-4005  
Fax: (267) 930-4771  
Email: jsjohnson@mullen.law

426 W. Lancaster Avenue, Suite 200  
Devon, PA 19333

June 16, 2021

**VIA U.S. MAIL**

Consumer Protection Bureau  
Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Leaders Life Insurance Company (“Leaders Life”) located at 1350 South Boulder Avenue W, #900, Tulsa, Oklahoma 74119, and are writing to notify your office of an incident that may affect the security of certain personal information relating to two (2) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Leaders Life does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On November 27, 2020, Leaders Life Insurance Company (“Leaders Life”) learned that it was the target of a cybercriminal attack and that portions of its computer network were infected with malware. Leaders Life immediately took systems offline and, with the assistance of third-party forensic specialists, launched an investigation to determine the nature and scope of the incident. The investigation confirmed that certain folders on Leaders Life’s systems may have been accessed or removed from its systems without authorization between November 25 and November 27, 2020. Leaders Life therefore undertook a lengthy and time-intensive, thorough review of the potentially impacted folders and its internal files and systems in order to identify the information that was potentially impacted and to whom it related. In connection with this review, on or about December 11, 2020, a third-party firm was engaged to programmatically and manually review the large volume of files at issue to identify impacted individuals and the types of data associated with those individuals. Concurrently, Leaders Life internally reviewed their databases. and, on or about March 31, 2021, first determined that one or more of the potentially impacted folders included protected information related to individuals.

In conjunction and collaboration with the third-party review team, Leaders Life continued to diligently review the information and reconcile the information with its internal records in furtherance of identifying

Mullen.law

the individuals to whom the data relates and the appropriate contact information for those individuals. These efforts were completed on or around May 19, 2021, at which time Leaders Life determined the scope of impacted individuals and the types of protected data associated with those individuals as a result of the extensive internal review. The investigation determined that the information that may have been potentially affected includes name, date of birth, Tax ID number, and/or Social Security number.

Leaders Life thereafter worked to provide notification to potentially impacted individuals as quickly as possible. Importantly, there is no indication that any specific information was accessed or misused. However, Leaders Life notified potentially impacted individuals out of an abundance of caution.

#### **Notice to New Hampshire Residents**

On or about June 16, 2021, Leaders Life began providing written notice of this incident to affected individuals, which includes two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached hereto as *Exhibit A*.

#### **Other Steps Taken and To Be Taken**

Upon discovering the event, Leaders Life moved quickly to investigate and respond to the incident, assess the security of Leaders Life systems, and notify potentially affected individuals. Leaders Life is also working to implement additional safeguards and training to its employees. Further, Leaders Life is providing access to credit monitoring services for twenty-four (24) months, through TransUnion to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Leaders Life will also be notifying other regulatory authorities, as required.

Additionally, Leaders Life is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

#### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4005.

Very truly yours,



Julie Siebert-Johnson of  
MULLEN COUGHLIN LLC

JSJ:rrg  
Enclosure

# Exhibit A



Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>>

<<Date>>

Re: Notice of Data <<Event/Breach>>

Dear <<Name 1>>:

At Leaders Life Insurance Co (“Leaders Life”), we understand that the confidentiality of your information is very important, and we are committed to protecting it. We are writing to make you aware of an incident that may affect the security of some of your personal information. This letter provides details of the incident, our response, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

**What Happened?** On November 27, 2020, Leaders Life learned that it was the target of a cybercriminal attack and that portions of our computer network were infected with malware. We immediately took systems offline and, with the assistance of third-party forensic specialists, launched an investigation to determine the nature and scope of the incident. The investigation confirmed that certain folders on our systems may have been accessed or removed from our systems without authorization between November 25 and November 27, 2020. We therefore undertook a lengthy and time-intensive, thorough review of the potentially impacted folders and our internal files and systems in order to identify the information that was potentially impacted and to whom it related. In connection with this review, on or about December 11, 2020, a third-party firm was engaged to programmatically and manually review the large volume of files at issue to identify impacted individuals and the types of data associated with those individuals. Concurrently, Leaders Life internally reviewed their databases and, on or about March 31, 2021, first determined that one or more of the potentially impacted folders included protected information related to individuals.

In conjunction and collaboration with the third-party review team, Leaders Life continued to diligently review the information and reconcile the information with its internal records in furtherance of identifying the individuals to whom the data relates and the appropriate contact information for those individuals. These efforts were completed on or around May 19, 2021, at which time Leaders Life determined the scope of impacted individuals and the types of protected data associated with those individuals as a result of the extensive internal review.

We thereafter worked to provide notification to potentially impacted individuals as quickly as possible. **Importantly, there is no indication that your specific information was accessed or misused. However, we are notifying potentially impacted individuals out of an abundance of caution.**

**What Information was Involved?** Our investigation determined that the information related to you that may have been potentially affected includes your name, date of birth, Tax ID number, and/or Social Security number.

**What We Are Doing.** Information security is one of Leaders Life’s highest priorities, and we have strict security measures in place to protect information in our care. Upon discovering this incident, we immediately took steps to respond, including taking steps to mitigate the event by resetting passwords across the network and bringing in third-party forensic specialists to assist with the investigation and remediation. Further, we notified law enforcement of this event, and have been cooperating with their investigation. We reviewed existing security policies and have implemented additional cybersecurity measures to further protect against similar cybersecurity criminal attacks moving forward. We are notifying the appropriate regulatory authorities and all potentially impacted individuals, including you, so that you may take steps to protect your information.

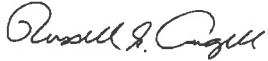
As an added precaution, we are offering you access to credit monitoring and identity theft protection services for 24 months through TransUnion, at no cost to you. You will find information on how to enroll in these services in the enclosed "*Steps You Can Take to Help Protect Your Information.*" We encourage you to enroll in these services as we are not able to do so on your behalf.

***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 information contained in the enclosed "*Steps You Can Take to Help Protect Your Information.*"

***For More Information.*** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 855-866-8963, which is available Monday - Friday, 9 a.m. to 9 p.m. Eastern.

We take this incident very seriously and sincerely regret any inconvenience or concern this incident caused you.

Sincerely,



Russ Angell  
Chief Operating Officer  
Leaders Life Insurance Co.

(Enclosure)

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### **Enroll in the Complimentary Monitoring Services**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

### **How to Enroll: You can sign up online or via U.S. mail delivery.**

- To enroll in this service, go to the *myTrueIdentity* website at [www.MyTrueIdentity.com](http://www.MyTrueIdentity.com) and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, three-bureau credit monitoring service via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode <<Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

### **ADDITIONAL DETAILS REGARDING YOUR COMPLIMENTARY CREDIT MONITORING SERVICE:**

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian®, and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

### **Monitor 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 your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 1-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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
1-888-298-0045	1-888-397-3742	1-833-395-6938
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**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; [www.identitytheft.gov](http://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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your 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](mailto: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 [www.oag.state.md.us](http://www.oag.state.md.us). Leaders Life is located at 1350 South Boulder Avenue W #900 Tulsa, Oklahoma 74119.

*For New Mexico residents*, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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](http://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](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are no Rhode Island residents impacted by this incident.