EVERSHEDS SUTHERLAND

Eversheds Sutherland (US) LLP
700 6th St. NW, Washington DC 20001
D: +1 202.383.0882

michaelbahar@eversheds-sutherland.com

July 6, 2022

Office of the Attorney General of Iowa
Hoover Building, 1305 E Walnut St,
Des Moines, IA 50319

Re: Data Security Event:

Dear Attorney General Miller,

Heritage Life Insurance Company is submitting this notice to provide the Attorney General of Iowa with information regarding a cybersecurity event at one of its service providers that impacted consumer personal information ("PI") of Iowa residents.

Heritage is a US life insurance company licensed in 49 states, Puerto Rico and the District of Columbia. Included within the corporate structure of Heritage are U.S. Financial Life Insurance Company ("USFLI") and Professional Life & Casualty Company ("PLCI"), which Heritage acquired in April 2020 and June 2019, respectively (together, "Heritage"). All of the Heritage companies are domiciled in Arizona. This notice is being provided on behalf of all three Heritage entities.

Heritage is a small business by head-count, employing 31 individuals, nearly half of whom joined following the acquisition of USLFI and PLCI. Heritage contracts with an IT provider, Inline Networks Integration LLC ("Inline"), to provide managed IT and network services.

On March 12, 2022, Inline informed Heritage that it had experienced a ransomware attack, which disrupted Heritage's customer call center and Heritage's systems for processing transactions and related data (e.g. redemptions, surrenders, beneficiary changes, etc.). While Inline's systems were down, Heritage worked to process transactions manually to the extent possible and communicate with policyholders about the system outage. Heritage's systems gradually came back online. The system hosting Heritage policy information was unavailable between March 12 and March 17, but it was accessible by March 18. The call center became operational on March 25, and Heritage was able to complete the processing of its backlogged transactional data by April 14. With the exception of the business days between March 14 and March 24, Heritage's customer support remained functional and in communication with Heritage customers throughout the outage as email and phones were not affected.

The ransomware attack did not affect Heritage's internal systems, including its policy administration system, and Heritage does not yet fully know which data sets the attack encrypted and which Inline simply took offline in response to the attack.

Throughout the course of this incident, Heritage, through counsel, has been in contact with Inline, and has communicated the urgent need to ascertain what, if any, Heritage customer data the attackers accessed. While Inline reports through its counsel that it engaged an incident response firm, they are not sharing the report with us, nor have they provided a full accounting of how the system was compromised, what data was accessed, what forensic artifacts have been preserved, and what steps were taken to remediate the issue.

For its part, Heritage took a number of steps to prevent further harm, including promptly retaining outside counsel with cybersecurity expertise, contacting law enforcement and regulators, undertaking its own internal forensic review, and eventually provided notice of contract termination to Inline. Heritage contacted the US Secret Service (USSS) on March 21, 2022, and on March 24, 2022 USSS requested Heritage not disclose the event to avoid interfering with their investigation. Heritage last communicated with the USSS on April 29, at which point the USSS no longer expressed concern with moving forward with notifications. To date, Inline has made no notifications to our knowledge.

Based on Heritage's own internal IT investigation, as well as on the limited information Inline has provided, Heritage assesses that customer PI was impacted. Whether that PI was actually accessed, exfiltrated or otherwise acquired remains unknown—Inline would be in the position to provide such an assessment based on their forensic investigation—but some systems that were encrypted contained personal information. Based on its ongoing investigation, on June 9, Heritage identified at least 961 Iowa residents whom this incident could have impacted.

Heritage is continuing to communicate with Inline, and it will update you and other regulatory agencies as the parallel investigations progress. In the interim, Heritage is erring on the side of being over-inclusive in determining who may have been affected, and it is working to ensure that affected individuals are notified with alacrity.

Should you have any questions please do not hesitate to contact me or Alexander Sand (AlexanderSand@eversheds-sutherland.com or +1.512.721.2721).

Sincerely,

Michael Bahar
Partner
Eversheds Sutherland (US) LLP

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

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

Subject: <<Variable Text 1>>

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a recent data security incident experienced by Inline Network Integration, LLC ("Inline") that may have involved your information. Inline takes the privacy and security of your information very seriously. This communication is being provided to you out of an abundance of caution, as we have no evidence that your personal information has been used inappropriately. Inline is the managed services provider "("MSP") for <<Inline Customer Name>>. <<Inline Customer Name>> data was being hosted on Inline's network at the time of the incident. Please read this letter carefully as it contains background information about the incident, the type of information involved, and steps you can take to protect your information.

What Happened? On March 12, 2022, Inline became aware of unusual activity within its digital environment. Upon discovering this activity, Inline immediately took steps to secure its network. Inline engaged leading cybersecurity firms to conduct an investigation to determine whether personal information hosted on its network may have been impacted as a result of the incident. The investigation revealed that an unauthorized actor may have acquired some Inline customer data including <<Inline Customer Name>> data. On <<date>>, we determined that some of your personal information may have been involved in this incident. Out of an abundance of caution, we are writing to inform you of the incident and to provide you with access to complimentary credit monitoring and identity protection services.

What Information Was Involved? The information impacted in connection with this incident may have included your name and <<Variable Text 2>>.

What Are We Doing? As soon as Inline discovered the incident, we took the measures described above. We also reported the incident to the FBI's Internet Crime Complaint Center. In addition, we are providing you with information about steps that you can take to help protect your personal information, and as an added precaution, we are offering you a <<one/two>>-year membership to TransUnion Interactive's myTrueIdentity credit monitoring and identity restoration service at no cost to you through Epiq. This product provides you with premier credit monitoring and identity theft resolution, including up to $1 million of identity theft insurance coverage. To receive these services, you must be over the age of 18, 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. The deadline to enroll is <<deadline>>.

What Can You Do? You can follow the recommendations included with this letter to help protect your information. Specifically, we recommend that you review your credit report for unusual activity. If you see anything that you do not understand or that looks suspicious, you should contact the consumer reporting agencies for assistance using the contact information included with this letter. In addition, you can enroll in the free credit monitoring services that we are offering to you through Epiq. Enrollment instructions are included with this letter.

For More Information: Further information about how to protect your personal information is included with this letter. If you have any questions regarding the incident or would like assistance with enrolling in the credit

sand identity monitoring services, please call 866-324-2812 between 9am to 9pm Eastern Time from Monday to Friday.

We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

[Signature]

Nichole Janner
Chief Operations Officer
Inline Network Integration, LLC

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, especially over the next 12 to 24 months, 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 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 http://www.annualcreditreport.com.

Security Freeze: In some U.S. 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: 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 may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Michigan Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	525 W Ottawa Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	P.O. Box 30213
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	Lansing, MI 48909
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	517-335-7622
1-877-438-4338			

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.