TRANSAMERICA®

Via Email

April 23, 2024

Re: Notice of Cybersecurity Event

Dear Sir/Madam,

Transamerica Life Insurance Company ("TLIC"), a financial services company with offices at 6400 C Street SW, Cedar Rapids, Iowa, 52499, is a licensee in Maryland. I am writing to provide notice of a security incident involving a vendor of TLIC.

No TLIC Information Systems have been compromised.

WebTPA Employer Services, LLC ("WebTPA") is a third party administrator (TPA) for claims adjudication for Transamerica Life Insurance Company for certain products. The information provided herein is based on our current understanding. In the event that WebTPA provides us with a revised data file, we will update this notice to the extent there are any material changes to the information provided herein.

Please see below for additional information.

(1) Date of the Cybersecurity Event

On December 28, 2023, WebTPA detected evidence of suspicious activity on the WebTPA network. WebTPA launched an investigation with support from industry leading third-party cybersecurity experts, IBM X-Force. WebTPA notified the FBI on January 27, 2024. Through its investigation, WebTPA determined that the unauthorized actor initially accessed the WebTPA network on March 6, 2023 through a VPN connection. The last evidence of attacker activity was May 12, 2023.

On January 29, 2024, WebTPA notified TLIC that our data may have been impacted.

(2) Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of Third-Party Service Providers, if any

Based on information provided by WebTPA, we understand that an unauthorized actor accessed the WebTPA ("Vendor") network through a VPN connection. WebTPA determined that the unauthorized actor initially accessed the WebTPA network on March 6, 2023 through a VPN connection. The last evidence of attacker activity was May 12, 2023.

(3) How the Cybersecurity Event was discovered

On January 29, 2024, WebTPA notified TLIC of WebTPA's cyber security incident. No confirmation of impacted TLIC data was received until data validation was completed. The data validation was completed on April 1, 2024.

(4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done

Any information that may have been exfiltrated by the threat actor was not recovered by WebTPA.

(5) The identity of the source of the Cybersecurity Event

Unknown.

(6) Whether Licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided

We understand from WebTPA, they notified the FBI on January 27, 2024.

(7) Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information or types of information allowing identification of the Consumer

Information included name, address, date of birth, social security number, subscriber number, member number, individual identification number and employee identification number.

(8) The period during which the Information System was compromised by the Cybersecurity Event

No TLIC Information Systems were compromised. Based on information from WebTPA, WebTPA determined that the unauthorized actor initially accessed the WebTPA network on March 6, 2023 through a VPN connection. The last evidence of attacker activity was May 12, 2023.

(9) The number of total Consumers in this State affected by the Cybersecurity Event. The Licensee shall provide the best estimate in the initial report to the Commissioner and update this estimate with each subsequent report to the Commissioner pursuant to this section

The incident involved the personal information of approximately 552 Maryland residents.

(10) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed

On April 19, 2024, per WebTPA, their internal review remains ongoing.

(11) Description of efforts being undertaken to remediate the situation which permitted the Cybersecurity Event to occur

Based on information provided by WebTPA, WebTPA has advised that it has made enhancements to security, disabled the domain admin account used by the unauthorized actor, and blocked known malicious IP addresses. WebTPA also forced a password reset for users in the affected network, updated its VPN appliance, enabled Halcyon Ransomware Protection Enforcement across the enterprise, and deployed CrowdStrike's Falcon EDR to further secure the WebTPA network from unauthorized access.

(12) A copy of the Licensee's privacy policy and a statement outlining the steps the Licensee will take to investigate and notify Consumers affected by the Cybersecurity Event

A copy of TLIC's privacy policy can be found at: https://www.transamerica.com/privacy-policy and https://www.transamerica.com/sites/default/files/files/e070d/hipaa-notice-privacy-practices_0.pdf.

WebTPA conducted the investigation regarding this event, as the attack was on WebTPA network (not on TLIC systems). According to WebTPA, WebTPA is offering affected individuals access to credit monitoring and identity restoration services through Kroll/Experian to potentially affected individuals. These services include fraud consultation and identity theft restoration services. There will be no cost to individuals for these services, but potentially affected individuals will need to complete the activation process. Information about these services and activation instructions are contained in the letter mailed to potentially affected individuals. TLIC is working with WebTPA to identify and notify impacted consumers and we anticipate that notices will be provided on or around May 15, 2024, by first class mail.

(13) Name of a contact person who is both familiar with the Cybersecurity Event and authorized to act for the Licensee.

Leanne Kopral, Assistant General Counsel
Transamerica
1801 California St., Suite 5200,
Denver, CO 80202
Telephone: 303-383-5867
Email: leanne.kopral@transamerica.com

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

<<first_name>> <<last_name>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>

Re: Notice of Data Breach

Dear <<first_name>>,

WebTPA Employer Services, LLC ("WebTPA") recently detected a data security incident impacting certain systems on our network. We are in possession of your information because we provided administrative services to benefit plans and insurance companies, including Transamerica Life Insurance Company. Some of your information may have been impacted in this incident. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing in response.

~~[[*For Data Owners that choose to be named in this letter, the second sentence above will read:* We are in possession of your information because we provided administrative services to benefit plans and insurance companies, including <<variable text (Data Owner's name)>>.]]~~

What happened?

On December 28, 2023, we detected evidence of suspicious activity on the WebTPA network that prompted us to launch an investigation. Upon detecting the incident, we promptly initiated measures to mitigate the threat and further secure our network. We also launched an investigation with the support of industry leading third-party cybersecurity experts and notified federal law enforcement.

The investigation concluded that the unauthorized actor may have accessed and/or obtained personal information between April 18 and April 23, 2023. In the course of the investigation, we determined that your information may have been impacted in this incident. WebTPA promptly informed your benefit plan or insurance company about the incident and the potential exposure of your information. We then diligently worked to confirm the individuals' impacted data and their contact information, which we provided to benefit plans and insurance companies.

What information was involved?

The information about you that may have been impacted includes: <<variable text (data elements)>>.

What are we doing?

WebTPA is offering two years of complimentary identity monitoring services through Kroll, including credit monitoring, fraud consultation, and identify theft restoration services. To take advantage of these free identity monitoring services, please follow the instructions in Attachment A. You must activate by <<variable text (activation date)>> to receive these services.

We deployed additional security measures and tools with the guidance of third-party cybersecurity experts to further strengthen the security of our network.

What can you do?

WebTPA is not aware of any misuse of your information as a result of this incident. Your financial information, such as financial account information or credit card numbers, was not involved in this incident. It is always advisable to remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing credit reports and Explanations of Benefits ("EOBs") from your benefit plans for suspicious activity. If you identify suspicious activity, you should contact the entity that maintains the information on your behalf. Additional information about how to help protect your information is contained in Attachment B.

For more information:

WebTPA has established a dedicated call center to answer questions. If you have any questions regarding this incident or the identity monitoring services available to you, please call TFN Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

Lisa Tranberg

President, WebTPA

Attachment A - Identity Monitoring Services

We have secured the services of Kroll to provide free identity monitoring 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.

How to Activate Your Complimentary Identity Monitoring Services

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

You have until <<variable text (activation date)>> to activate your complimentary identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your complimentary identity monitoring services, you can visit **info.krollmonitoring.com**. Additional information describing your services is included with this letter.

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.

Take Advantage of Your Complimentary 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.

Attachment B – Information for U.S. Residents

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)

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 https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:
equifax.com
equifax.com/personal/credit-report-services
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Experian:
experian.com
experian.com/help
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion:
transunion.com
transunion.com/credit-help
P.O. Box 1000
Chester, PA 19016
888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for one year. 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies 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 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. Identity theft victims and active-duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Additional Information

If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

For Iowa residents: ~~You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state Attorney General.~~ For Iowa residents, you are advised to report any suspected identity theft to law enforcement or to the Office of the Attorney General of Iowa, 1305 E Walnut St, Des Moines, IA 50319, 515-281-5926 or 1-888-777-4590, https://www.iowaattorneygeneral.gov/ . Information regarding placing a security freeze on your credit report is available at https://www.iowaattorneygeneral.gov/for-consumers/general-consumer-information/identity-theft/security-freeze-identity-theft.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

For Massachusetts residents: You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New York residents: For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at http://www.dos.ny.gov/consumerprotection or (800) 697-1220 or NYS Attorney General at http://www.ag.ny.gov/home.html or (800) 771-7755.

For New Mexico Residents: You have rights pursuant to the FCRA, 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 FCRA, 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 violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA 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 Avenue NW, Washington, DC 20580.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the FTC and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Commercial Services website at www.dfcs.oregon.gov/id_theft.html and click "How to get a security freeze."

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, you have the right to obtain any police report filed in regard to this event.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, Washington, D.C., and West Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).