
Good afternoon. Please see the below information regarding a security breach impacting one Maryland resident.

--

Company: Gerber Life Insurance Company

Brief description of the nature of the security breach: On February 21, 2024, WebTPA, one of the third-party administration partners of Gerber Life Insurance Company ("Gerber Life"), provided Gerber Life notification of a data security incident at WebTPA involving unauthorized access to its network via a VPN connection. The incident resulted in unauthorized access to the claim data of individuals enrolled in Gerber Life group student accident insurance administered by WebTPA. On March 27, 2024, Gerber Life received the findings of WebTPA's concluded investigation. In cooperation with WebTPA, Gerber Life is in the process of providing written notice to impacted individuals and, where required, notifying the appropriate regulatory authorities pursuant to applicable state laws.

The number of Maryland residents being notified (also attach a sample copy of the notice being sent to consumers): 1 (please find sample attached). Written notice will be provided to the Maryland resident; the approximate mail date is 5/8/2024.

What information has been compromised: Name, DOB, Subscriber Number, Member ID No. and Individual ID No.

Any steps the business is taking to restore the integrity of the system: WebTPA promptly launched an investigation, initiated measures to mitigate the threat, determine what had taken place and how and further secure their network. They employed the support of industry leading third-party cybersecurity experts, notified federal law enforcement and are offering two years of complimentary identity monitoring services to those impacted by the incident.

--

Please feel free to contact me directly if there are any additional questions, comments or concerns.

Thank you.

Jamoki Hamilton JD, CIPP/US, CRISC
Compliance Manager – Privacy & Information Security Governance

1311 Mamaroneck Ave, Suite 350, White Plains, NY 10605
914.259.4222 direct

gerberlife.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 Gerber 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.

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 on March 27, 2024.

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 identity 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](https://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 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).