NOTICE OF DATA PRIVACY EVENT

July 22, 2026 — Risk Program Administrators (“RPA”) is providing notice of a recent data security event that may have affected personal information related to certain individuals. While RPA is unaware of any actual or attempted identity fraud in relation to the incident, it is providing potentially affected individuals with information about the incident and steps individuals may take to help protect against the possible misuse of their information.

What Happened? RPA became aware of suspicious activity related to an employee’s email account. We quickly took steps to secure the account and launched an investigation into the nature and scope of the incident with the assistance of external cybersecurity experts. The investigation determined that an unknown authorized person gained access to certain emails on or about May 27, 2025 to June 16, 2025.

Following this investigation and with the assistance of external specialists, we conducted a comprehensive review of the information that may have been accessed during this time period. Although we do not have any evidence that information has been misused, we have determined that certain information relating to individuals could have been accessed by the unknown unauthorized person, as identified below.

What Information Was Affected? The affected data varies by individual but includes full name, address, Social Security number, driver’s license number, date of birth, financial account information, medical information and health insurance information including: treatment type, treatment location, treatment cost, physician information, mental or physical condition, subscriber member number, admission date.

How Will Individuals Know If They Are Affected By This Incident? RPA is in the process of mailing notice letters to individuals whose protected information was contained within the files at issue and for whom it has valid mailing address information.

What Affected Individuals Can Do. As a precautionary measure, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing their account statements, credit reports, and explanations of benefits for unusual activity and to detect errors. Any suspicious activity should promptly be reported to the appropriate insurance company, health care provider, or financial institution. Interested individuals can also review the *Steps You Can Take to Help Protect Your Information* below for further guidance.

For More Information. If you have questions, please call our dedicated assistance line at 1-888-202-4124 (toll free), Monday through Friday, from 8am - 8pm Central Time (excluding U.S. holidays). You may also write to RPA at P.O. Box 989728, West Sacramento, CA 95798-9728.

Steps You Can Take to Help Protect Your Information

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 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 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 their 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.