OFFICE OF THE LIQUIDATOR OF
PHYSICIANS STANDARD INSURANCE COMPANY

November 26, 2024

Notice of Data Security Incident

This is notice of a data security incident involving the electronic records of Physicians Standard Insurance Company ("**PSIC**") and certain affiliates. PSIC is an insolvent medical malpractice insurer in liquidation pursuant to a Final Order and Judgment of Liquidation entered by the District Court of Shawnee County, Kansas, effective December 1, 2019. The Liquidator of PSIC, Kansas Commissioner of Insurance, Vicki Schmidt (the "**Liquidator**"), is providing this notice to alert those whose personal information may have been impacted.

What Happened. We have learned from the vendor storing PSIC's servers that a criminal actor gained unauthorized access to the PSIC servers, encrypted the data, and is holding the data ransom.

What We Are Doing. Fortunately, the Liquidator has a backup of the data that was stored to the servers. However, it would be costly, with no result guaranteed, to hire a cyber security firm to try to confirm which data the criminal actor accessed, whether it was in a format that would be usable, and whether the criminal wrongfully distributed the data. The estimated cost to identify and provide notice to potentially affected consumers exceeds $100,000.00. As an alternative to the costly and uncertain endeavor of confirming whether the criminal actor accessed personally identifiable information and identifying those affected, we are providing notice of the data breach via the Liquidator's website for PSIC at https://insurance.kansas.gov/legal-issues/#psic, and statewide media outlets in Kansas and Missouri as authorized by applicable Kansas and Missouri statutes.[1]

Information Involved. The data included the following types of information: names, basic contact information, summaries of claimant allegations which contain medical information and some medical records of claimants; potential social security numbers, tax identification numbers, license numbers; and information used for payments, *e.g.*, ACH information.

What You Can Do. We are not aware of any individual's information being misused as a result of the incident, but as a precautionary measure, we encourage you to take steps to ensure your data remains secure. We recommend you remain vigilant for incidents or suspicious activity of identity theft or fraud by review of bank accounts and other financial statements. You can follow the recommendations on the following pages to help protect your personal information. For your security, please note that we will not initiate contact with you regarding this cybersecurity incident by phone call, text, or email. Should someone unexpectedly initiate contact with you by phone, email or text regarding this incident, you should end the phone call or delete any text or email as a security precaution. We encourage you to remain vigilant against incidents of identity theft and fraud, promptly change any potentially involved account passwords, and to proactively review account statements, credit reports, and explanation of benefits forms for suspicious activity.

Access to Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228 (toll-free). You may also contact the three major credit bureaus directly to request a free copy of your credit report. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Request a Security Freeze. You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a security freeze to control who may access 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 security freeze on your credit report. To request a security freeze, you must provide the following information:

1. Full name (including middle initial as well as Jr., Sr. II, III, etc., if applicable)
2. Social Security number
3. Date of birth
4. Each address where you have lived over the past five (5) years
5. A legible photocopy of a government-issued identification card (a state driver's license or ID card, military identification, etc.)
6. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Placing a Fraud Alert. As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a one-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 lasts seven (7) years.

To access your credit report, implement a security freeze, or a fraud alert, you may contact the three major credit reporting agencies listed below.

	Credit Report	Security Freeze	Fraud Alert
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/help/credit-freeze/	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/fraud/center.html
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze	P.O. Box 2000 Chester, PA 19016-2000 1-800-680-7289 www.transunion.com/fraud-alerts

For any additional questions or concerns, you may contact us by email at kdoi.psic@ks.gov. The Federal Trade Commission can be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with the Federal Trade Commission. You can obtain further information on how to file such a complaint via the contact information listed above. You have the right to file a police report if you do experience identity theft or fraud. To file a report with law enforcement for identity theft, you may need to provide some proof that you have been victimized. You should report instances of known or suspected identity theft to law enforcement and your state Attorney General.

[1] See Mo. Rev. Stat. § 407.1500.2(7) and K.S.A. 50-7a01(e).