Physicians Insurance
A MUTUAL COMPANY
MedChoice
RISK RETENTION GROUP

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

30051

FIRST_NAME MI LAST_NAME SUFFIX
company
ADDRESS1
ADDRESS2
CITY, state zip

July 18, 2023

Notice of Data Security Incident

Dear First_Name Mi Last_Name Suffix:

Physicians Insurance A Mutual Company is writing to inform you of a data security incident that may have exposed your personal information to unauthorized persons. Although we have no evidence to suggest that any of your personal information has been misused, we are reaching out to provide additional information and an opportunity to enroll in free credit monitoring.

Physicians Insurance A Mutual Company, its affiliate MedChoice Risk Retention Group, Inc., and its subsidiary Experix, LLC (collectively "Physicians Insurance"), provide professional liability insurance for physicians, clinics, facilities, and hospitals in Alaska, Idaho, Oregon, and Washington. Physicians Insurance also operates and reinsures MedChoice Risk Retention Group, Inc, which provides professional liability insurance for physicians, clinics, facilities, and hospitals on a national basis. Physicians Insurance's subsidiary, Experix, LLC, provides third party claims administrator services to MedChoice and other captives and risk retention groups.

WHAT HAPPENED

On March 2, 2023, Physicians Insurance identified access to an employee's work email account by an unknown third party. Upon discovery, we immediately shut down the mailbox and reset passwords, which terminated the access. We also promptly initiated an investigation and hired third party cybersecurity experts to assist in investigating the source and scope of the activity. We subsequently determined that the access was isolated to a single user's email account and only lasted approximately an hour on March 2, 2023 before that access was terminated. We did not find any evidence that indicates that any emails or attachments were exported from the user's email account, but we have not been able to confirm whether the files that contained personal information were actually accessed or viewed by the third party. Therefore, we cannot say with certainty if any of your information in those files was accessed or viewed. Nevertheless, in an abundance of caution, we are providing this notice to alert you to the potential that your information was accessed as part of this incident.

WHAT INFORMATION WAS INVOLVED

The information that the unknown third party may have been able to access may have included: full name, contact information, date of birth, government identification (such as your Social Security or driver's license number), and financial information (such as your bank account number but not any security or access code related to that account).

WHAT WE ARE DOING

We have security measures in place that allow us to take prompt action against attempted intrusions into our systems. Those measures were implemented here and reduced the scope of the third party's activity. We also hired third party experts to address this situation, perform an investigation into the unauthorized activity, and further secure our systems to help protect the information we maintain. This notice was not delayed by a law enforcement investigation.

WHAT YOU CAN DO

Enclosed with this letter you will find additional steps you can take to protect yourself.

In addition, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by: date** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code: code**

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at 877-288-8057 by **date** and provide them with the engagement number **engagement number**.

FOR MORE INFORMATION

We have established a toll-free call center to support you and answer your questions about the incident and this notice. You can contact the call center at 866-985-2484, and one of our representatives will be happy to assist you. Thank you for your understanding and patience, and we regret any inconvenience this incident may cause.

Sincerely,

Melissa Cunningham
General Counsel and Sr. Vice President
Physicians Insurance A Mutual Company
MedChoice Risk Retention Group
601 Union Street, Suite 500
Seattle, WA 98101

PHYSIN-ADT-2-CONCM

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling 1-877-322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider notifying your Attorney General, local law enforcement, or the Federal Trade Commission. You can also file a police report concerning the suspicious activity and request a copy of that report.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft. For any services not described above, please be aware that the consumer reporting agencies may charge you a fee.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For North Carolina Residents: the North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents: the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; 1-800-771-7755; www.ag.ny.gov.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit:
https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Physicians Insurance A MUTUAL COMPANY | MedChoice RISK RETENTION GROUP

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

FIRST_NAME MI LAST_NAME SUFFIX
company
ADDRESS1
ADDRESS2
CITY, state zip

July 18, 2023

Notice of Data Security Incident

Dear First_Name Mi Last_Name Suffix:

Physicians Insurance A Mutual Company is writing to inform you about a data security incident that may have exposed your personal health information to unauthorized persons. Although we have no evidence to suggest that any of your personal health information has been misused, we are reaching out in an abundance of caution to provide notice to alert you to the potential that your information was accessed as part of this incident.

Physicians Insurance A Mutual Company, its affiliate MedChoice Risk Retention Group, Inc., and its subsidiary Experix, LLC (collectively "Physicians Insurance"), provide professional liability insurance for physicians, clinics, facilities, and hospitals in Alaska, Idaho, Oregon, and Washington. Physicians Insurance also operates and reinsures MedChoice Risk Retention Group, Inc, which provides professional liability insurance for physicians, clinics, facilities, and hospitals on a national basis. Physicians Insurance's subsidiary, Experix, LLC, provides third party claims administrator services to MedChoice and other captives and risk retention groups.

WHAT HAPPENED

On March 2, 2023, Physicians Insurance identified access to an employee's work email account by an unknown third party. Upon discovery, we immediately shut down the mailbox and reset employee passwords, which terminated the access. We also promptly initiated an investigation and hired third party cybersecurity experts to assist in investigating the source and scope of the activity. We subsequently determined that the unauthorized access was isolated to a single user's email account and only lasted approximately an hour on March 2, 2023 before the access was terminated. We did not find any evidence to indicate that any emails or attachments were exported from the user's email account, but we have not been able to confirm whether the files that contained personal information were accessed or viewed by the third party. Therefore, we cannot say with certainty if any of your information in those files was accessed or viewed. Nevertheless, in an abundance of caution, we are providing this notice to alert you to the potential that your information was accessed as part of this incident.

WHAT INFORMATION WAS INVOLVED

The information that the unknown third party may have been able to access may have included: full name, date of birth, contact information, medical treatment information, or health insurance information.

WHAT WE ARE DOING

We have security measures in place that allow us to take prompt action against attempted intrusions into our systems. Those measures were implemented here and reduced the scope of the third party's activity. We also hired third party experts to address this situation, perform an investigation into the unauthorized activity, and further secure our systems to help protect the information we maintain. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

We encourage you to remain vigilant for incidents of fraud and identity theft by reviewing your account statements (if any) and monitoring free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your financial institutions or company with which the account is maintained, as well as applicable authorities, including local law enforcement, your state attorney general and the Federal Trade Commission ("FTC"). Enclosed with this letter you will find additional steps you can take to protect yourself. If you have questions about this matter, please call us at the phone number below.

FOR MORE INFORMATION

We have established a toll-free call center to support you and answer your questions about the incident and this notice. You can contact the call center at 866-985-2484, and one of our representatives will be happy to assist you. Thank you for your understanding and patience, and we regret any inconvenience this incident may cause.

Sincerely,

Melissa Cunningham
General Counsel and Sr. Vice President
Physicians Insurance A Mutual Company
MedChoice Risk Retention Group
601 Union Street, Suite 500
Seattle, WA 98101

PHYSIN-ADT-2-NOCM

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling 1-877-322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider notifying your Attorney General, local law enforcement, or the Federal Trade Commission. You can also file a police report concerning the suspicious activity and request a copy of that report.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft. For any services not described above, please be aware that the consumer reporting agencies may charge you a fee.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For North Carolina Residents: the North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents: the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; 1-800-771-7755; www.ag.ny.gov.

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 incident. There is 1 Rhode Island resident impacted by this incident.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.