



Secure Processing Center  
25 Route 111, P.O. Box 1048  
Smithtown, NY 11787

<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<City>>, <<State>> <<Zip>>

<<Date>>

## NOTICE OF <<VARIABLE DATA 1>>

Dear <<Full Name >>:

Premier Health Partners (“Premier Health”) is writing to inform you of an incident that may have impacted the security of some of your information, which is in our possession due to your relationship with one or more of the following organizations: Miami Valley Hospital, Atrium Medical Center, and Upper Valley Medical Center, which are owned by Premier Health. We are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

**What Happened?** On July 12, 2023, we became aware of suspicious activity related to certain systems within the Premier Health environment. We immediately launched an investigation to determine the nature and scope of the activity with the assistance of third-party forensic specialists. Our investigation determined that files on certain Premier Health systems were subject to access and acquisition by an unauthorized party at varying times between June 7, 2023 and July 12, 2023. In response, Premier Health began reviewing the affected systems to determine what, if any, sensitive information was contained within the systems in question. Following this time-consuming process, Premier Health determined certain information related to you may have been contained within the files.

**What Information Was Involved?** The following types of your information may have been included in the files: your name and date of birth, Social Security number, driver's license number or state issued identification number, passport number, individual taxpayer identification number, digital signature, login credentials, financial account information, medical information, and health insurance information.

**What We Are Doing.** Premier Health takes the confidentiality, privacy, and security of information in our care very seriously. Upon discovery, Premier Health immediately commenced an investigation to confirm the nature and scope of the incident. Premier Health reported this incident to law enforcement, has implemented additional layers of security, and is taking steps to implement additional safeguards and review policies and procedures relating to data privacy and security.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Information*.

**For More Information.** Premier Health understands you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call our dedicated assistance line at 855-507-7876, between the hours of 9:00am and 9:00pm (Eastern Time), excluding holidays. You may also write to Premier Health, Privacy Office, 110 North Main Street, Suite 300, Dayton, OH 45402.

We apologize for any inconvenience that has been caused by this event.

Sincerely,

Premier Health Partners

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### Enroll in Monitoring Services



<<Full Name >>

Enter your Activation Code: <<Activation Code>>

Enrollment Deadline: <<Enrollment Deadline>>

Service Term: <<CM Duration>>Months\*

### Medical Shield Complete

#### Key Features

- 1-Bureau Credit Monitoring
- Health Insurance Plan Number Monitoring
- Medical Record Number Monitoring
- Medical Beneficiary Identifier Monitoring
- National Provider Number Monitoring
- International Classification of Diseases Monitoring
- Health Savings Account Monitoring
- Dark Web Monitoring
- Victim Assistance
- \$1 Million Identity Theft Insurance\*\*

#### Enrollment Instructions

To enroll in Medical Shield, visit [app.medicalshield.cyex.com/enrollment/activate/php](http://app.medicalshield.cyex.com/enrollment/activate/php)

1. Enter your unique Activation Code <<Activation Code>>

Enter your Activation Code and click 'Redeem Code'.

2. Create Your Account

Enter your email address, create your password, and click 'Create Account'.

3. Register

Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.

4. Complete Activation

Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Medical Shield code will no longer be active. If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Medical Shield, so please enroll before the deadline. If you need assistance with the enrollment process or have questions regarding Medical Shield, please call Medical Shield directly at 1 866.622.9303.

---

\*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

\*\*Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## **Monitor Your Accounts**

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](http://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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/databreach-help">https://www.transunion.com/databreach-help</a>
1-888-298-0045	1-888-397-3742	1-833-799-5355
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 your 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](http://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.

*For District of Columbia residents*, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and [oag.dc.gov](http://oag.dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

*For New Mexico residents*, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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 Ave. N.W., Washington, D.C. 20580.

*For New York residents*, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.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](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.