



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

RECEIVED

JUL 05 2024

DEPT. OF CONSUMER  
AFFAIRS

Postal Endorsement Line  
<<Full Name>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<City>>, <<State>> <<Zip>>  
<<Country>>  
\*\*\*Postal IMB Barcode

<<Date>>

**NOTICE OF <<VARIABLE DATA 2>>**

Dear <<Full Name>>,

SouthCoast Medical Group, LLC (“SouthCoast Health”) and Privia Medical Group of Georgia, LLC (“Privia”) are writing to notify you of an incident that may impact the privacy of some of your personal information. Please note that this incident only occurred within SouthCoast Health’s network. Privia’s network was not affected by this incident. SouthCoast Health takes this incident very seriously and is providing you with information about the incident, our response to it, and resources we are making available to you to help protect your information, should you feel it appropriate to do so.

**What Happened?** On June 18, 2023, SouthCoast Health became aware of unauthorized activity within our network. In response, we promptly took steps to secure our systems and investigate the nature and scope of the event with assistance from third-party forensic specialists. The investigation determined that between June 15 - June 18, 2023, an unauthorized actor gained access to our network and viewed or copied certain files stored on certain systems. We identified the involved files and undertook a comprehensive and time-consuming review to identify sensitive information, the individuals to whom it relates, and address information to be used for notifying impacted individuals. This review was recently completed on June 13, 2024, and your information was determined to be involved.

**What Information Was Involved?** While we have no indication of identity theft or fraud in relation to this incident, our review determined that the following types of your information were present in the affected files: <<Data Elements>><<Variable Data 1>> and name. Please note that SouthCoast Health’s electronic medical record (EMR) systems were not impacted by this event.

**What Are We Doing?** The confidentiality, privacy, and security of personal information within our care is among our highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to secure our systems and performed a full investigation. We have implemented additional security measures to further protect against similar incidents moving forward. We notified federal law enforcement of this incident and are cooperating with their investigation. We are also notifying applicable regulators, including the U.S. Department of Health and Human Services.

Additionally, we are offering credit monitoring and identity theft protection services for <<CM Duration>> months through CyEx, at no cost to you. Please note that you will not be automatically enrolled in these services. Should you wish to do so, you will need to enroll yourself in these services, as we are not able to do so on your behalf. You may find instructions on how to enroll in these services in the enclosed *Steps You Can Take to Help Protect Personal Information*.

**What Can You Do?** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements 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 Personal Information*. There you will also find more information on the complimentary credit monitoring and identity protection services we are making available to you, free of cost.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions or need assistance, please call our dedicated assistance line at 888-596-7145 between the hours of 9:00am - 9:00pm, Eastern Time, Monday through Friday (excluding major U.S. holidays).

We sincerely regret any inconvenience or concern this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,



John Marrero  
Chief Executive Officer  
SouthCoast Medical Group, LLC

## STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

### Enroll in Credit Monitoring and Restoration



<<Full Name>>

Enter your Activation Code: XXXXXXXXXX  
Enrollment Deadline: <<Enrollment Deadline>>  
Service Term: <<CM Duration>> months \*

### Identity Defense Complete

#### Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance\*\*

#### Enrollment Instructions

To enroll in Identity Defense, visit [app.identitydefense.com/enrollment/activate/southcoast](https://app.identitydefense.com/enrollment/activate/southcoast)

- 1. Enter your unique 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 Identity Defense code will no longer be active. If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense 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 your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the 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 credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

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 you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, 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/credit-help">https://www.transunion.com/credit-help</a> |
| 1-888-298-0045  | 1-888-397-3742  | 1-800-916-8800  |
| Equifax Fraud Alert, P.O. Box 105069<br>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<br>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**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your 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, DC 20001; 202-727-3400; 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; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

*For New Mexico residents*, you have rights pursuant to the Fair Credit Reporting Act, 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 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 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 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 you to review your 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, you have the right to obtain any police report filed in regard to this incident. There are <<RI Count>> Rhode Island residents impacted by this incident.