PruittHealth
FAMILY MAKES US STRONGER

May 30, 2024

Return Mail Processing
PruittHealth Compliance Department
1626 Jeurgens Court
Norcross, GA 30093

L3593-L02-0000002 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L02
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY

RE: Notice of Data Security Incident

Dear PruittHealth Family:

The purpose of this letter is to provide written notice of a data security incident that potentially involves your protected health information, or that of another for whom you are a personal representative. This notice is provided to you as required by the Health Insurance Portability and Accountability Act of 1996 (more commonly known as "HIPAA"); specifically, this notice is provided pursuant to 45 C.F.R. § 164.404(a)(1) and 45 C.F.R. § 164.404(d)(1).

The circumstances of this incident are summarized as follows. In November of 2023, PruittHealth discovered that certain of its computer network resources had been attacked by illegal foreign actors, commonly known as "hackers." In immediate response, PruittHealth took steps to ensure the security of its network and to remove the hackers from the network. This included the engagement of third-party forensic specialists to assist with securing the environment and investigating the extent of the hackers' activity.

During the course of our forensic investigation, it was determined that the hackers may have removed copies of a number of electronic files that had been stored on a common file server. The hackers threatened to publish the stolen files on a "dark web" blog site unless PruittHealth paid the hackers money as ransom.

On December 7, 2023, the hackers claimed to have published the files that they allegedly copied on their blog site. However, before PruittHealth's forensic specialists could access the files the hackers claim to have published, the hackers' blog site was taken down and any files that they claimed to have published were no longer accessible. As a result, PruittHealth is not able to confirm whether your information was exposed.

We have performed extensive reviews of the files that were contained on the server at issue, and there is the possibility that some information related to your individual information, including potentially full or partial name, date of birth, government identification information, demographic information, contact information, home address, financial information including, Social security numbers, bank account number, health insurance information, and health information, may have been affected. While we have no evidence confirming that your information was taken, it is nevertheless possible that an unauthorized third party could have obtained this information. Therefore, we encourage you to review the attachment to this letter for additional information and steps to take with respect to potential identity theft.

Please be on the lookout for any scams that ask you to provide your personal information in connection with this incident. We will NOT call you or send you any email messages asking for your personal information or credit card information in relation to this incident or send you any email messages asking you to "click" on any links to activate identity protection services. You should not provide information in response to any such calls or email messages, and you should not click on any links within any such email messages.

We sincerely apologize and regret that this incident has occurred, and we understand that this may pose an inconvenience to you. PruittHealth is committed to providing quality care, including the protection of your personal information. We maintain high standards for the safeguarding of protected health information and take all potential or actual security incidents seriously. In response to this incident, PruittHealth is taking steps to prevent recurrence of similar incidents, which include the ongoing investigation and work by our Information Systems Department enhance our privacy and security practices as well as the technical protection of our data.

Thank you for your attention to this notice. If you have questions or would like additional information, you can email us at compliance@pruitthealth.com, or by regular mail to PruittHealth, Compliance Department, 1626 Juergens Court, Norcross, GA 30093, or find more information at: https://www.pruitthealth.com/.

Sincerely,

Richard E. Gardner III
Chief Compliance Officer

Attachment

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Please consider taking the steps set forth below as an additional precaution to protect yourself from identity theft.

1. **Credit Reports.** Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annualreport-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact one of the three major credit bureaus to place a fraud alert on your credit report.

Equifax	**Experian (TRW)**	**TransUnion Corp**
P.O. Box 740241	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

When you receive a copy of your credit report, you should examine it closely for evidence of fraud, such as the presence of credit accounts that you have not opened. Please note that the credit bureaus may require a power of attorney, letters of guardianship or conservatorship, or other documentation from your next of kin/family member for them to be able to speak on your behalf.

2. **Fraud Alerts**. A fraud alert can help prevent an identity thief from opening a new credit account in your name. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As soon as the credit bureau that you contact confirms the fraud alert, the other two credit bureaus will automatically be notified also to place fraud alerts on your information. Once a fraud alert is implemented, you are entitled to order one free copy of your credit report (as described above) from each of the three nationwide consumer reporting companies.

3. **Credit Freezes.** You may also have the option of instituting a "credit freeze" or "security freeze" on your credit file. A security freeze locks your credit file so that no one will be able to access your data (or improperly open an account in your name) without your permission. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit.

For Georgia Residents: Georgia citizens who are victims of identity theft or 65 years of age or older are eligible for a security freeze free of charge.

4. **Contact the Federal Trade Commission (FTC) and State Attorneys General Offices**. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338). Finally, you may also want to review the webpage from the Federal Trade Commission that sets forth strategies for recovering from identity theft, which is available here: https://identitytheft.gov.

5. State Specific Resident Information:

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office

Bureau of Internet and Technology

(212) 416-8433

https://ag.ny.gov/internet/resource-center

NYS Department of State's Division of Consumer Protection

(800) 697-1220

https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge but note that consumer reporting agencies may charge fees for other services.