LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Tara Aaron-Stelluto
3102 West End Avenue, Suite 400
Nashville, TN 37203
Tara.Stelluto@lewisbrisbois.com
Direct: 615.439.2689

September 23, 2022

VIA ONLINE SUBMISSION
Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

We represent Physician's Business Office, Inc. ("PBO"), a Parkersburg, West Virginia-based company that provides medical practice management and administrative services for healthcare providers. We are writing to notify you that PBO experienced a data security incident that may have affected the personal information of 4 Maine residents. PBO is taking this matter extremely seriously and has implemented several security measures to help prevent such an incident from happening again.

1. **Nature of the Security Incident.**

In April 2022, PBO became aware of unusual activity in its network environment. PBO immediately took steps to secure its network and hired an independent digital forensics and incident response firm to assist. PBO subsequently determined that certain information on PBO's systems had been accessed and potentially acquired by an unauthorized actor during the incident. Some of the potentially affected information included files PBO maintained on behalf of healthcare providers in the course of its services. PBO then undertook a comprehensive review of the potentially affected data to determine whether any personal or protected health information was impacted, to confirm the healthcare providers to which the data pertained, and to discern the identities of any individuals whose data may have been involved. PBO completed those efforts on June 30, 2022 and notified each provider about the incident and the potential impact to individual patients' data on July 26, 2022. After obtaining the providers' consent to issue notifications on their behalf, PBO worked to collect current mailing addresses for potentially impacted individuals. PBO completed that process on September 16, 2022 and arranged for notification letters to be sent as soon as possible thereafter.

2. Number of Maine Residents Affected.

PBO will be notifying 4 potentially affected Maine residents via first class U.S. mail on September 23, 2022, via the attached notification letter template, or a substantially similar version thereof. The potentially affected personal information for Maine residents may include name, home address, date of birth, Social Security number, driver's license number, medical treatment and diagnosis information, disability code, prescription information and health insurance account information.

3. Steps Taken Relating to the Incident.

As soon as PBO discovered this incident, it took steps to secure its environment and enlisted an external cybersecurity firm for assistance. PBO has also implemented additional safeguards to help ensure the security of its network and to reduce the risk of a similar incident occurring in the future.

PBO has established a toll-free call center through IDX to answer questions about the incident and address related concerns. In addition, PBO is offering 12 months of complimentary credit and identity monitoring services to the potentially affected Maine residents.

4. Contact Information.

PBO remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 615.439.2689 or via email at Tara.Stelluto@lewisbrisbois.com.

Very truly yours,

Tara Aaron-Stelluto of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

Encl.: Sample Consumer Notification Letter

Physician's BUSINESS OFFICE

P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
(833) 423-2939
Or Visit:
https://response.idx.us/pbo
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zipcode>>

September 23, 2022

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a data security incident experienced by Physician's Business Office, Inc. ("PBO"), that may have involved your personal and protected health information. PBO provides medical practice management and administrative services for <<Variable Text 1 - Provider>>. The privacy of individuals' information is very important to PBO. That is why I am writing to notify you of this incident and to provide information about steps you can take to help protect your information.

What Happened? In April 2022, PBO became aware of unusual activity within its computer environment. After taking steps to secure its network with the help of its information technology provider, PBO hired a leading, independent digital forensics and incident response firm to investigate what happened and to help identify whether any sensitive information may have been involved. PBO subsequently determined that certain information on PBO's computer systems may have been accessed or acquired by an unknown individual, including personal and protected health information in files that PBO maintained in the course of its services for <<Variable Text 2 - Provider Short Name>>. PBO worked diligently to identify the potentially affected individuals and to collect up-to-date mailing addresses for purposes of providing notification. PBO completed that process on June 30, 2022, and provided notice of the incident to <<Variable Text 2 - Provider Short Name>> on July 26, 2022. After consulting with <<Variable Text 2 - Provider Short Name>>, PBO arranged for this letter to be sent. PBO is not aware of any misuse of the information that may have been impacted.

What Information Was Involved? The information that may have been involved in this incident includes your name, home address, date of birth, Social Security number, driver's license number, medical treatment and diagnosis information, disability code, prescription information and health insurance account information.

What Are We Doing? As soon as PBO discovered the incident, it took the steps described above, including hiring an external cybersecurity firm to conduct an investigation. PBO has also implemented several measures in its computer system to increase the security of the information it stores and reduce the likelihood of a similar incident happening again. In addition, we are offering you complimentary credit monitoring and identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Please note that the deadline to enroll is December 23, 2022.

What You Can Do: PBO encourages you to follow the recommendations at the end of this letter to help protect your information. We also encourage you to contact IDX with any questions and to enroll in the free credit monitoring and identity protection services by calling (833) 423-2939 or going to https://response.idx.us/pbo and using the Enrollment Code provided above.

For More Information: If you have any questions about this letter, please call (833) 423-2939, Monday through Friday from 9 am - 9 pm Eastern Time. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding the protection of your information.

PBO is taking this matter extremely seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Jeff Matheny, President
Physician's Business Office, Inc.

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf
1-877-438-4338

West Virginia Attorney General
Consumer Protection & Anti-Trust Division
P.O. Box 1789
Charleston, WV 25326
Fax: (304) 558-0184

Ohio Office of the Attorney General
Attorney General Dave Yost
Consumer Protection Division
30 E Broad Street, 14th Floor
Columbus, OH 43215

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
877-566-7226 (Toll-free within North Carolina)
919-716-6000

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

California Department of Justice
Office of the Attorney General
Attn: Public Inquiry Unit
P.O. Box 944255
Sacramento, CA 94244-2550

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. 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.