LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsey Smith
100 Light Street, Suite 1300
Baltimore, Maryland 21202
Lindsey.Smith@lewisbrisbois.com
Direct: 410.525.6402

February 23, 2022

File No. 39395.439

VIA E-MAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

I represent Dr. Douglas C. Morrow ODPC ("Dr. Morrow"), headquartered in Auburn, Indiana, with respect to a recent data security incident described in greater detail below. Dr. Morrow takes the protection of sensitive information very seriously and is taking steps to prevent similar incidents from occurring in the future.

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

On May 16, 2021, Dr. Morrow experienced an encryption attack. Dr. Morrow immediately began investigating the incident and retained digital forensics professionals to determine what happened and whether information may have been accessed or acquired without authorization. On October 29, 2021, the investigation determined that the attacker gained access to Dr. Morrow's data and may have acquired protected health information. On December 8, 2021, Dr. Morrow identified individuals whose protected personal information may have been compromised. The impacted information may have included names, addresses, health insurance information, and medical information.

2. **Number of Maryland Residents Affected.**

Dr. Morrow notified six (6) residents of Maryland via first class U.S. mail on February 23, 2022. A sample copy of the notification letter sent to the affected individuals is included with this correspondence.

3. Steps Taken Relating to the Incident.

Dr. Morrow is not aware of any fraudulent activity relating from this incident. Dr. Morrow has taken the steps described above in response to this incident, including retaining cybersecurity professionals to assist with responding to the incident. Additionally, Dr. Morrow implemented additional safeguards to help ensure the security of its digital environment and to reduce the risk of a similar incident occurring in the future.

4. Contact Information.

Dr. Morrow 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 410.525.6402 or via email at Lindsey.Smith@lewisbrisbois.com.

Sincerely,

Lindsey Smith of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LS
Encl.: Consumer Notification Letter Template

VISION SOURCE™

P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-676-2192
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [XXXXXXXX]

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

February 23, 2022

Re: Notice of <<Variable Text 1>>

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

I am writing to inform you of a data security incident experienced by Dr. Douglas C. Morrow ODPC ("Dr. Morrow"), that may have affected your personal information, to offer you complimentary credit monitoring and identity protection services, and to inform you about steps that can be taken to help protect your personal information.

What Happened? On May 16, 2021, Dr. Morrow detected unusual activity that impacted access to systems and data. Upon discovering this activity, we took steps to secure the environment and launched an investigation to determine the extent of the incident. Additionally, we engaged a digital forensics firm to assist with the investigation and help assess whether any sensitive information may have been accessed or acquired without authorization. On October 29, 2021, the investigation concluded that, between May 13 and 15, an unauthorized actor accessed Dr. Morrow's systems and data and may have acquired patient information. Following this discovery, we conducted a comprehensive review of the contents of the impacted systems to determine what, if any, sensitive data might have been affected. On December 8, 2021, we discovered that the incident may have impacted your information. Although there is no evidence that your information has been misused, out of an abundance of caution, we are notifying you about this incident and offering complimentary credit monitoring and identity protection services as described in more detail below.

What Information Was Involved? The information involved may have included: <<Variable Text 2>>.

What We Are Doing. As soon as we discovered this incident, we took the measures referenced above to secure the impacted systems and investigate the incident. We also implemented measures to help prevent a similar incident from occurring in the future. In addition, we are offering identity theft protection services through IDX, the 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 id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

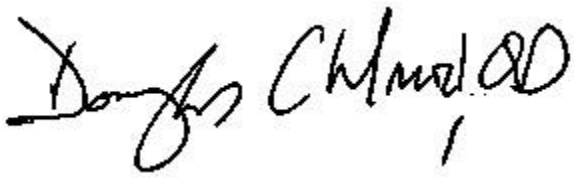
What You Can Do. Please read the recommendations included with this letter which you can follow to help protect your personal information. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-676-2192 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 a.m. to 9 p.m. Eastern Time. Please note the deadline to enroll is May 23, 2022.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information: If you have questions or need assistance, please call 1-833-676-2192, Monday through Friday from 9 a.m. to 9 p.m. Eastern Time. Please have your Enrollment Code ready.

Protecting your information is important to us. Please know that we take this incident very seriously and deeply regret any worry or inconvenience that this may cause you.

Sincerely,



Douglas C. Morrow, OD

Steps You Can Take to Further Protect Your 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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-909-8872	1-888-397-3742	1-800-685-1111	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	www.annualcreditreport.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 90 days. 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: Under U.S. law, 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. Contact information for the FTC is: **Federal Trade Commission,** 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov and www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General Bureau of Internet and Technology Resources	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
28 Liberty Street	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
New York, NY 10005	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
ifraud@ag.ny.gov	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
1-212-416-8433	1-888-743-0023	1-877-566-7226	401-274-4400

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 others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf

Enrollment in IDX Identity Protection

Website and Enrollment. Please visit **https://app.idx.us/account-creation/protect** and follow the instructions for enrollment using your Enrollment Code included with this letter.

Activate the credit monitoring provided as part of your IDX membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at **1-833-676-2192** to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

This IDX enrollment will include:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - IDX fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDX Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.